CA IdentityMinder™

Versionshinweise

r12.6.1

Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden.

Diese Dokumentation darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden. Diese Dokumentation enthält vertrauliche und firmeneigene Informationen von CA und darf vom Nutzer nicht weitergegeben oder zu anderen Zwecken verwendet werden als zu denen, die (i) in einer separaten Vereinbarung zwischen dem Nutzer und CA über die Verwendung der CA-Software, auf die sich die Dokumentation bezieht, zugelassen sind, oder die (ii) in einer separaten Vertraulichkeitsvereinbarung zwischen dem Nutzer und CA festgehalten wurden.

Ungeachtet der oben genannten Bestimmungen ist der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2013 CA. Alle Rechte vorbehalten. Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber.

CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA Technologies:

- CA IdentityMinder ™
- CA SiteMinder®
- CA Directory
- CA User Activity Reporting (CA UAR)
- CA CloudMinder™ Identity Management
- GovernanceMinder (früher bezeichnet als CA Role & Compliance Manager)

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 1: Neue Funktionen 9

12.6.1 9
- Neue Zertifizierungen 9
- SSL-fähiger JNDI-Benutzerspeicher 10
- Unterstützung mobiler Apps 10

12.6 11
- Neuer Name und Anzeige 11
- Vereinfachte Benutzererfahrung 12
- Bereitstellungs-Verbesserungen 12
- Connector-Verbesserungen 13
- Leistungs-Verbesserungen 14
- Policy Xpress-Verbesserungen 16
- Sichere Management-Konsole 17
- Basiszugriffsanfragen 17
- Neue Dokumentation für Config Xpress 19
- Systemeigener CA IdentityMinder-Ersatz für SiteMinder Advanced Password Services 20
- Dynamische Schlüssel für das Verschlüsseln von Daten 21
- Synchronisierung von Active Directory-Servern 21
- Auditing von Anmelde- und Abmeldeereignissen 21
- SHA-2 22

Kapitel 2: Hinweise zur Installation 23

Unterstützte Plattformen und Versionen 23
Veraltete und verworfene Komponenten 23
JDK-Anforderung für Linux-Installationen 24
Nicht verschlüsselte Kennwörter 24
Oracle Oracle 11g R2 RAC als Benutzerspeicher und Objektspeicher 24
ADAM 2008 als Benutzerspeicher 24
Nicht-ASCII-Zeichen verursacht Installationsfehler auf nicht englischsprachigen Systemen 25
Installation des Bereitstellungsverzeichnisses auf Linux 25
Identity Manager-EAR wird nicht automatisch mit WebLogic bereitgestellt 26
Umgehen der Firewall unter Windows 2008 SP2 26
Bereitstellen von JSP-Seiten für Administratoraktionen 26
CA IdentityMinder auf Linux 64-Bit mit SiteMinder-Konnektivitätsfehlern 27
Verbessern der Leistung bei WebSphere und AIX 28
Ignorieren von WebSphere 7/Oracle-Fehlern 28

Kapitel 3: Upgrades 29

Unterstützte Upgrade-Pfade 29
Neue Active Directory-Rollendefinitionsdatei 30
Aktualisieren auf die Datei "jboss.xml" 30
64-Bit-Anwendungsserver 31
Problem beim Upgrade eines Clusters von CA IdentityMinder r12 CR6 oder einer späteren Version 31
Upgrade von r12.5 SP6 oder älter auf WebLogic 32
Fehler bei der Umgebungsmigration 33
Upgrade-Fehler von Credential Provider 33
Interner Fehler des Vista Credential Providers 33
Kein Suchfenster mit der Aufgabe "Durchsuchen und Korrelieren" 34
Nicht schwerwiegender Fehler nach dem Upgrade des Bereitstellungsmanagers von r12 34
Umbenennen von ACF2-, RACF- und TSS-Endpunkten vor dem Upgrade 35

Kapitel 4: Bekannte Probleme 37

Allgemein 37
- Bereitstellungsverzeichnis lässt sich nicht über die Management-Konsole erstellen 37
- AttributeLevelEncryption für Benutzerkennwörter 38
- Spezifizieren von LDAP-DN bei Verwendung von TEWS 39
- Fehler mit "setpasswd" bei 64-Bit-Linux-Systemen 39
- Problem mit Kennwortrichtlinien bei Verwendung eines kombinierten Benutzerspeicher- und Bereitstellungsverzeichnisses 40
- Verbindung zum CA IdentityMinder-Server kann nicht hergestellt werden, wenn der Kennwortsynchronisierungs-Agent für 64-Bit-Active Directory konfiguriert wird 41
- Workflow-Teilnehmer-Resolver schlägt für EnableUserEventRoles fehl 42
- Doppelter Name in "Gesendete Aufgaben anzeigen" 42
- Fehlermeldung "Nicht gefunden" beim Erstellen einer neuen Umgebung in manchen Bereitstellungen 42
- Ändern von zusammengesetzten Attributen mit einzelnem Wert im Identity Manager 43
- Beschränkungen des Massendatenladers auf Beziehungsattribut-Ebene 44
- Fehler beim Erstellen einer bereitstellungsaktivierten Umgebung mithilfe von Token-Vorlagen 44
- Voraussetzungen für Oracle-Anwendungen 44
- Oracle 11gR2 RAC-Benutzerspeicher: Groß- und Kleinschreibung bei der Suche 45
- CA IdentityMinder unter JBoss nimmt Verbindung zu Oracle nicht wieder auf 45
- Fehler bei "Zum Hauptinhalt wechseln" in Mozilla Firefox 46
- Fehler bei gleichzeitigen Änderungen an einem Benutzer 46
- Änderung an Policy Xpress-Syntax 46
- Aktualisieren gemäß SAP-Hilfethema 47

Berichterstellung 47
- Bei der Benutzerfiltersuche ist in den Benutzerkonten und den XML-Dateien zu benutzerdefinierten Snapshots der Endpunktkonten die Groß-/Kleinschreibung zu beachten. 47
- Satisfy=All funktioniert in XML-Datei nicht ordnungsgemäß 47

Problem beim Verwenden mehrerer Filter auf Endpunktobjekten 48
Snapshot erfasst keine Gruppenobjektdaten 48
Allgemein 48
Umbenennen von Bereitstellungsrollen wird nicht unterstützt 48
Solaris ECS-Protokollierung oberhalb der INFO-Ebene kann die Leistung des Bereitstellungsservers verringern 48
Fehler "Bereits vorhanden" beim Hinzufügen eines Endpunkts 49
Fehler bei der Korrelation eines Microsoft SQL-Endpunkts 49
Einschränkung beim SiteMinder-Anmeldenamen für globalen Benutzernamen 50
CA IAM CS und Connector Xpress 50
JNDI-Kontoverwaltungsfenster – das Erstellen von Konten mit mehreren strukturierten Objektklassen schlägt fehl 50
Endpunkttypen 50
Allgemein 50
Zugriffssteuerung 53
CA Arcot 55
Active Directory 55
CA SSO für den Connector des Servers für erweiterte Richtlinien 56
DB2 und DB2 für z/OS 56
E2Kx 57
Google Apps 58
PeopleSoft 60
SAP 60
Siebel 61

Kapitel 5: Behobene Probleme 63

12.6.1 63

Kapitel 6: Dokumentation 65

Bookshelf 66
Versionshinweise für CA IdentityMinder- und CA RCM-Integration 66

Anhang A: Barrierefreiheitsfunktionen 67

508 Compliance 67
Produktverbesserungen 67

Kapitel 1: Neue Funktionen

Dieses Kapitel enthält folgende Themen:

12.6.1 (siehe Seite 9)
12.6 (siehe Seite 11)

12.6.1

Neue Zertifizierungen (siehe Seite 9)

SSL-fähiger JNDI-Benutzerspeicher (siehe Seite 10)

Unterstützung mobiler Apps (siehe Seite 10)

Neue Zertifizierungen

Die folgenden neuen Plattformen sind mit CA IdentityMinder r12.6.1 zertifiziert:

Endpunkte

- Microsoft SQL 2012 als statischer und dynamischer Endpunkt
- CA Directory r12 SP10 CR2 als JNDI-Endpunkt
- CA Embedded Entitlements Manager (EEM) - unterstützt vom Bereitstellungsmanager

CA IdentityMinder-Benutzerspeicher

- CA Directory r12 SP10 CR2

CA IdentityMinder-Benutzerspeicher und Laufzeitspeicher

- Microsoft SQL Server 2012

Zusätzliche Unterstützung

- Mozilla Firefox 14.x
- BusinessObjects Report Server XI 3.1 SP5 (CA Business Intelligence 3.3)

  Diese Version stimmt mit der von CA SiteMinder unterstützten Version überein
- Unterstützung des Report Server in Hochverfügbarkeitskonfigurationen
- Unterstützung von CA IdentityMinder mit CA GovernanceMinder (CA RCM) r12.6
- Unterstützung von CA IdentityMinder mit CA SiteMinder r12.0 SP3 CR11

SSL-fähiger JNDI-Benutzerspeicher

Peer-Zertifikatsprüfung wird derzeit durchgeführt. Bei dieser Funktion müssen Sie das SSL-Serverzertifikat des Benutzerspeichers dem CA IdentityMinder-JRE-Standardschlüsselspeicher hinzufügen. Der Schlüsselspeicher ist die Cacerts- oder Jssecacerts-Datei an folgendem Speicherort:

JAVA_HOME\jre\lib\

Unterstützung mobiler Apps

Die mobile CA IdentityMinder-App befähigt Sie, Ihre bestehende CA IdentityMinder-Infrastruktur so einzusetzen, dass Benutzer die folgenden Aufgaben über ein mobiles Gerät wie einem iPhone oder iPad ausführen können:

- Zurücksetzen von vergessenen Kennwörtern

  Hinweis: Wenn Sie mobilen Benutzern ermöglichen, ein vergessenes Kennwort über deren Gerät zurückzusetzen, verlässt sich CA IdentityMinder auf die Gerätesicherheit anstelle von Sicherheitsfragen. Möglicherweise muss die Gerätesicherheit erhöht werden, zum Beispiel durch einen Passcode, bevor Sie die Funktion zum Rücksetzen von Kennwörtern aktivieren.

- Ändern eines Kennworts
- Reagieren auf Genehmigungsanforderungen
- Anzeigen von Managerdetails

  Diese Funktion erlaubt Benutzern, die Workflow-Anfragen genehmigen, Informationen zum Vorgesetzten (Manager) eines Benutzers anzuzeigen.

Hinweis: Weitere Informationen zur mobilen App finden Sie im *Administrationshandbuch*.

12.6

Neuer Name und Anzeige (siehe Seite 11)

Vereinfachte Benutzererfahrung (siehe Seite 12)

Bereitstellungs-Verbesserungen (siehe Seite 12)

Connector-Verbesserungen (siehe Seite 13)

Leistungs-Verbesserungen (siehe Seite 14)

Policy Xpress-Verbesserungen (siehe Seite 16)

Sichere Management-Konsole (siehe Seite 17)

Basiszugriffsanfragen (siehe Seite 17)

Neue Dokumentation für Config Xpress (siehe Seite 19)

Systemeigener CA IdentityMinder-Ersatz für SiteMinder Advanced Password Services (siehe Seite 20)

Dynamische Schlüssel für das Verschlüsseln von Daten (siehe Seite 21)

Synchronisierung von Active Directory-Servern (siehe Seite 21)

Auditing von Benutzeranmelde- und Benutzerabmeldeereignissen (siehe Seite 21)

SHA-2 (siehe Seite 22)

Neuer Name und Anzeige

In dieser Version wurde CA Identity Manager in CA IdentityMinder umbenannt. Alle CA Security-Produkte werden umbenannt, um dem Namen der Produktfamilie "Minder" zu folgen. Diese Änderung vereinfacht die Identifizierung von CA Security-Produkten und betont die Zusammengehörigkeit der CA-Sicherheitslösungen.

Zusätzlich ist die Standardbenutzerkonsole aktualisiert worden, um neue CA-Stile und -Farben zu integrieren.

Java Connector Server (Java CS oder JCS) wurde in CA IAM Connector Server umbenannt (CA IAM CS).

Vereinfachte Benutzererfahrung

Diese Version schließt die folgenden Verbesserungen an der Benutzererfahrung ein:

- Aktualisierte Fenster für Self-Service-Aufgaben

  Die folgenden Fenster wurden aktualisiert, um die Benutzerfreundlichkeit zu verbessern:

  - Erscheinungsbild des Portals für das Anmeldefenster
  - Selbstregistrierung/Erstellung von Identität
  - Mein Kennwort ändern
  - Kennwort vergessen – Zurücksetzen
  - Benutzer-ID vergessen
- Bestimmte Admin-Aufgaben nutzen Web 2.0-Steuerelemente.

Bereitstellungs-Verbesserungen

CA IdentityMinder 12.6 schließt die folgenden neuen Funktionen und Änderungen zur Verbesserung der Bereitstellung ein.

Bereitstellungsserver unter Linux

Der Bereitstellungsserver kann jetzt unter Red Hat Linux als eine Alternative zu Solaris installiert werden.

Funktionen des Bereitstellungsmanagers in der Benutzerkonsole

Einige Funktionen des Bereitstellungsmanagers werden jetzt in der Benutzerkonsole unterstützt:

- Synchronisierung von Benutzern, Rollen, Endpunktkonten und Kontovorlagen

  Die Integration von Endpunkten und Konten in CA IdentityMinder kann zu Verlusten bei der Synchronisierung führen. Beispielsweise können sich die Bereitstellungsrollen oder Kontovorlagen, die einem Benutzer zugewiesen werden, von den tatsächlichen Konten für diesen Benutzer unterscheiden. Dieses Problem kann mit Synchronisierungsaufgaben behoben werden.
- Korrelationsregeln steuern die Zuordnung von Endpunktkontoattributen zu Benutzerattributen in der Benutzerkonsole. So hat beispielsweise Access Control ein Attribut namens "AccountName". Sie können eine Regel erstellen, um es "FullName" in der Benutzerkonsole zuzuordnen.

Connector-Verbesserungen

CA IdentityMinder 12.6 schließt die folgenden neuen Funktionen und Änderungen ein, mit deren Hilfe sich die Erstellung und Bereitstellung neuer Connectors vereinfacht.

Hot Deployment – Installieren eines neuen Connector ohne Neustart von CA IAM CS

CA IAM Connector Server (CA IAM CS) ist der neue Name für Java Connector Server (oder Java CS oder JCS).

CA IAM CS unterstützt jetzt *Hot Deployment*. Hot Deployment ist ein Prozess, mit dessen Hilfe eine Komponente ohne Neustart von CA IAM CS hinzugefügt, entfernt oder aktualisiert werden kann. Sie können jetzt die folgenden Aufgaben ausführen:

- Installieren, Deinstallieren oder Upgraden eines Connector *ohne* Neustart von CA IAM CS

  Sie können einen neuen oder aktualisierten Connector bereitstellen und installieren, ohne CA IAM CS neu zu starten oder sich bei seinem Host anzumelden. Wenden Sie sich an den CA Support für die neuesten Connector-Versionen.

- Bereitstellen von Bibliotheken anderer Anbieter ohne Neustart von CA IAM CS

  Einige Connectors benötigen Bibliotheken, die nicht im Lieferumfang von CA IAM CS sind. Bisher mussten Sie diese Bibliotheken bereitstellen und dann CA IAM CS neu starten. Jetzt können Sie diese Bibliotheken bereitstellen, während der Connector-Server ausgeführt wird.

  CA IAM CS enthält einen Kernsatz von Bibliotheken anderer Anbieter, und jeder Connector kann jede dieser Bibliotheken verwenden. Ein Connector kann auch andere Bibliotheken von Drittanbietern enthalten, die er benötigt.

Hinweis: Hot Deployment funktioniert nicht für C++-Connectors.

Bundle Builder – Neues Tool für das Erstellen von Connectors

CA IAM CS erfordert, dass Connectors als Open Services Gateway Initiative-Bundles geliefert werden. Das OSGi-Framework ist ein Modulsystem und eine Service-Plattform für die Java-Programmiersprache, die ein vollständiges und dynamisches Komponentenmodell implementiert. Das SDK für den Connector-Server schließt jetzt ein Bundle Builder-Tool ein, das Ihnen dabei hilft, Ihren Connector mit einem Bundle zu umgeben.

Anmelden für Connectors und CA IAM CS

Sie können sich jetzt bei CA IAM CS anmelden, um aktuellste Protokollmeldungen für CA IAM CS und seine Connectors zu sehen. Sie können weiterhin Protokolldateien verwenden, um alle Protokollmeldungen zu sehen.

Zertifikate für Connectors und CA IAM CS

Sie können sich jetzt bei CA IAM CS anmelden, um Zertifikate für CA IAM CS und seine Connectors anzuzeigen und zu verwalten.

Verwenden von Connector Xpress zum Zuordnen von benutzerdefinierten Attributen zu benutzerdefinierten Funktionsattributen

Verwenden Sie Connector Xpress, um benutzerdefinierte Attribute und benutzerdefinierte Funktionsattribute zuzuordnen. Die Zuordnung der Attribute kann nicht mehr über die XML-Datei "<jcs-home>/conf/override/lnd/lnd_custom_metatdata.xml" vorgenommen werden.

CA IAM CS ist ein Proxy für CCS

CA IdentityMinder verwendet jetzt CA IAM CS als einen Proxy für den C++ Connector Server (CCS). CA IdentityMinder kommuniziert nicht mehr direkt mit CCS.

Leistungs-Verbesserungen

CA IdentityMinder 12.6 bietet Leistungsverbesserungen in folgenden Bereiche des Produkts.

Verbesserung der Leistung des Massendatenladers

In dieser Version ist die Leistung des Massendatenladers verbessert. Die Verbesserungen schließen die folgenden Änderungen ein:

- Höhere Übermittlungsrate von Aufgaben durch die übergeordnete Massendatenlader (Feeder)-Aufgabe. Es können mehr Aufgaben parallel ausgeführt werden.
- Optimierungen bei der Wiederverwendung von Datenbankverbindungen; Zwischenspeicherung der Attributdefinitionen von verwalteten Objekten führt von Anfang bis Ende zu einer schnelleren Ausführung von Aufgaben.
- Verbesserungen an einigen Plug-ins und Listenern beschleunigt die Verarbeitung von Ereignissen, die während der Aufgabenausführung generiert werden.

Um die Leistung weiter zu verbessern, empfehlen wir, dass Sie für die Dauer des Massendatenladevorgangs folgende Änderung vornehmen:

- Deaktivieren Sie alle unerwünschten Policy Xpress-Richtlinien, Business Logic Task-Handler und Synchronisierungs-Flags auf Aufgabenebene.
- Führen Sie den Massendatenlader (Feeder) als dedizierter Benutzer mit möglichst wenigen Admin-Rollen und Admin-Aufgaben in Bereich aus.

Hinweis: Weitere Informationen zu zusätzlichen Leistungsverbesserungen finden Sie im Abschnitt zum Massendatenlader im *Administrationshandbuch*.

Verbesserte Snapshot-Exportleistung

Für diese Version wurde der Exportprozess von Snapshot-Daten für Berichte umgestaltet, um die Leistung und Benutzerfreundlichkeit zu verbessern. Mithilfe des Snapshot-Definitionsassistenten können Sie die Regeln zum Laden von Benutzern, Endpunkten, Admin-Rollen, Bereitstellungsrollen, Gruppen und Organisationen definieren oder anpassen.

Mithilfe dieser Funktion können Sie eine Benutzerkonsolen-Aufgabe verwenden, um nur die gewünschten Attribute auszuwählen und für eine bestimmte Snapshot-Instanz zu exportieren. In früheren Versionen mussten Benutzer eine XML-Datei manuell bearbeiten.

Hinweis: Sie können weiterhin die Standard-XML-Dateien für das Erfassen von Snapshots verwenden und anpassen.

Weitere Informationen zum Erstellen von Snapshot-Definitionen finden Sie im *Administrationshandbuch*.

Policy Xpress-Verbesserungen

Diese Version enthält die folgenden Verbesserungen von Policy Xpress:

- Attribut-Plug-ins für verwaltete Objekte

  Die folgenden Plug-ins für verwaltete Objektattribute sind zu Policy Xpress hinzugefügt worden:

  - Objekt Attribute – Erlauben Ihnen, den Wert eines verwalteten Objektattributs zu extrahieren.
  - Hat sich das Objektattribut geändert/Attribut eines bestimmten Objekts – Wie "Hat sich das Benutzerattribut geändert" und "Attribut eines bestimmten Benutzers", aber es kann jeder Typ von verwaltetem Objekt verwendet werden
  - Set Objekt Attribut – Erlaubt Ihnen, das Attribut von verwalteten Objekten zu ändern

- Kürzungsfunktion

  Die Kürzungsfunktion ermöglicht es Ihnen, unerwünschte voran- oder nachgestellte Bereiche aus Datenelementen oder Zeichenfolgen zu entfernen.

- Unterstützung für weitere Aktionsregeln

  Bisher konnten einer Richtlinie nicht mehr als 60–70 Aktionsregeln hinzugefügt werden, sonst hat Policy Xpress die ganze Richtlinie nicht hinzugefügt. In diesem Fall wurden weder ein Fehler noch eine Ausnahme in den Protokollen berichtet. Jetzt unterstützen Policy Xpress-Richtlinien bis zu 500 Aktionsregeln.

- Policy Xpress-Wiki

  Die Policy Xpress-Dokumentation wurde aktualisiert und befindet sich nun auf einem Wiki https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/wiki/-/wiki/Main/Policy+Xpress?&#p_36 in der CA Security Global User Community.

Sichere Management-Konsole

Die Management-Konsole ermöglicht Administratoren, CA IdentityMinder-Verzeichnisse und -Umgebungen zu erstellen und zu verwalten.

Die CA IdentityMinder-Installation enthält nun eine Option, die standardmäßig aktiviert ist und die der Sicherung der Management-Konsole dient. Während der Installation erstellen Sie ein Konto, das auf die Management-Konsole in einem vordefinierten Verzeichnis zugreifen kann.

Nach der Installation können Sie der Management-Konsole zusätzliche Administratoren hinzufügen, die einen Zugriff benötigen.

Hinweis: Weitere Informationen finden Sie im *Konfigurationshandbuch*.

Basiszugriffsanfragen

CA IdentityMinder-Benutzer können Zugriff auf Dienste anfordern, die sie zur Ausführung ihrer Arbeitsaufgaben benötigen.

Ein *Dienst* bündelt alle Berechtigungen (Aufgaben, Rollen, Gruppen und Attribute), die ein Benutzer für eine bestimmte Unternehmensrolle benötigt. Die Dienste sind für den Benutzer über Zugriffsanfrage-Aufgaben in der CA IdentityMinder-Benutzerkonsole verfügbar. Zugriffsanfrage-Aufgaben ermöglichen einem Benutzer oder Administrator, einen Service über die Benutzeroberfläche anzufordern, zuzuweisen, zu widerrufen und zu erneuern.

Dienste ermöglichen einem Administrator, Benutzerberechtigungen in einem einzigen Paket zu kombinieren, die dann als ein Set verwaltet werden. Zum Beispiel benötigen alle neuen Vertriebsmitarbeiter Zugriff auf einen definierten Satz von Aufgaben und auf Konten von bestimmten Endpunktsystemen. Sie benötigen auch bestimmte Informationen, die zu ihren Benutzerkontoprofilen hinzugefügt wurden. Ein Systemadministrator erstellt einen Service namens Vertriebsverwaltung, der alle erforderlichen Aufgaben, Rollen, Gruppen und Profilattributinformation für einen neuen Vertriebsmitarbeiter enthält. Wenn ein Administrator den Service "Vertriebsverwaltung" einem Benutzer zuweist, erhält dieser Benutzer die gesamte Gruppe an Rollen, Aufgaben, Gruppen und Kontoattributen, die vom Service definiert werden.

Eine weitere Möglichkeit, wie Benutzer auf Services zugreifen können, ist mit einer eigenen Zugriffsanfrage. In der Benutzerkonsole hat jeder Benutzer eine Liste von Services, die für seine Anfrage verfügbar sind. Diese Liste wird mit Services gefüllt, die von einem Systemadministrator mit den entsprechenden Berechtigungen als "Selbstabonnierend" markiert wurden, normalerweise während der Service-Erstellung. Über die Liste der verfügbaren Services können Benutzer den Zugriff auf die benötigten Services anfordern. Wenn der Benutzer Zugriff auf einen Service anfordert, wird die Anfrage automatisch erfüllt, und die zugeordneten Berechtigungen werden dem Benutzer sofort zugewiesen. Ein Administrator mit den entsprechenden Berechtigungen kann die Service-Abwicklung auch so konfigurieren, dass eine Workflow-Genehmigung erforderlich ist oder E-Mail-Benachrichtigungen generiert werden.

Hinweis: Diese Anfangsversion unterstützt Funktionen für Basiszugriffsanfragen. Die Zugriffsanforderungs-Funktionalität ermöglicht Endbenutzern, Berechtigungen anzufordern (verwaltet und nicht verwaltet von CA IdentityMinder), Genehmigungsabläufe zu definieren und Abwicklungsabläufe zu verwenden.

Diese Anfangsversion bietet keine Unterstützung für erweiterte Zugriffsanforderungsfunktionen wie

- Massendefinition von Zugriffsanforderungs-Dienstobjekten
- Integration von GovernanceMinder (früher Role and Compliance Manager genannt)
- Detailliertes Filtern und Suchen

Diese Anfangsversion bietet keine Unterstützung von folgenden Funktionen:

- Massendefinition von Dienstobjekten
- Detaillierte Filterung
- Suchen
- Integration von anderen Abwicklungsmechanismen

Weitere Informationen zu Diensten finden Sie im *Administrationshandbuch*.

Neue Dokumentation für Config Xpress

Config Xpress ist ein Tool, das mit CA IdentityMinder bereitgestellt wird. Sie können dieses Tool verwenden, um die Konfigurationen Ihrer CA IdentityMinder-Umgebungen zu analysieren und um mit diesen Konfigurationen zu arbeiten.

Config Xpress ermöglicht es Ihnen, folgende Aufgaben auszuführen:

- Verschieben von Komponenten zwischen Umgebungen.

  Das Tool entdeckt automatisch andere erforderliche Komponenten und fordert Sie auch dazu auf, diese zu verschieben. Dies kann Ihnen viel Arbeit ersparen.
- Veröffentlichen eines Berichts zu den Systemkomponenten in einer PDF-Datei.
- Veröffentlichen der XML-Konfiguration einer bestimmten Komponente.

Weitere Informationen zum Importieren von Konfigurationen finden Sie unter Verwalten der Konfiguration mit Config Xpress im *Konfigurationshandbuch*.

Systemeigener CA IdentityMinder-Ersatz für SiteMinder Advanced Password Services

Zusätzlich zu den grundlegenden Kennwortrichtlinien bietet CA IdentityMinder die folgenden zusätzlichen Kennworteinstellungen, die nun von SiteMinder abgekoppelt sind:

- Ablauf des Kennworts:
  - Verfolgen von fehlgeschlagenen oder erfolgreichen Anmeldungen – Wenn die Option aktiviert ist, werden Nachverfolgungsinformationen für erfolgreiche oder fehlgeschlagene Anmeldeversuche zum Kennwortdatenattribut des dazugehörigen Benutzers im Benutzerspeicher geschrieben.
  - Authentifizieren von Anmeldungsnachverfolgungsfehler – Wenn die Option deaktiviert ist, können sich Benutzer nur anmelden, wenn CA IdentityMinder Nachverfolgungsinformationen in den Benutzerspeicher schreiben kann.
  - Kennwort läuft ab, wenn es nicht geändert wird – Konfiguriert das Verhalten bei Ablauf. Wenn das Kennwort nach einer angegebenen Anzahl von Tagen nicht geändert wurde, werden Benutzer deaktiviert oder gezwungen, ihr Kennwort zu ändern. Erlaubt auch das Senden von Ablaufwarnungen nach einer angegebenen Anzahl von Tagen.
  - Kennwort-Inaktivität – Konfiguriert inaktives Benutzerverhalten. Wenn der Benutzer nach einer angegebenen Anzahl von Tagen keinen erfolgreichen Anmeldeversuch unternommen hat, werden Benutzer deaktiviert oder gezwungen, ihr Kennwort zu ändern.
  - Ungültiges Kennwort – Konfiguriert die Anzahl von fehlgeschlagenen Anmeldungen, die erlaubt sind, bevor der Benutzer deaktiviert wird.
  - Mehrere reguläre Ausdrücke – Gibt reguläre Ausdrücke an, mit denen Kennwörter übereinstimmen müssen bzw. nicht übereinstimmen dürfen. CA IdentityMinder-Kennwortrichtlinien unterstützen einen einzelnen Ausdruck von jedem Typ.
- Beschränkungen für Kennwort:
  - Mindestanzahl von Tagen vor Wiederverwendung
  - Mindestanzahl von Kennwörtern vor Wiederverwendung
  - Prozentualer Unterschied zum letzten Kennwort
  - Bei der Prüfung auf Unterschiede Sequenz ignorieren – Ignoriert beim Berechnen des prozentualen Unterschieds die Position von Zeichen.

Hinweis: Diese Version unterstützt keine historischen Kennwortdaten einer CA IdentityMinder-Bereitstellung, die CA SiteMinder Password Services (Kennwortverlauf) für Bereitstellungen verwendet, die nur CA IdentityMinder r12.6-Kennwortdienste umfasst.

Dynamische Schlüssel für das Verschlüsseln von Daten

In einer Umgebung können Sie dynamische Schlüssel erstellen, die Daten verschlüsseln oder entschlüsseln. Wenn Sie vermuten, dass ein Benutzer unbefugten Zugriff auf einen Schlüssel erhalten hat, können Sie das Kennwort für den Schlüsselspeicher ändern. Der Schlüsselspeicher ist die Datenbank für geheime Schlüssel. Sobald Sie dieses Kennwort ändern, verschlüsselt CA IdentityMinder die Werte der Schlüssel wieder.

Weitere Details dazu finden Sie im Abschnitt Geheime Schlüssel des *Administrationshandbuchs*.

Synchronisierung von Active Directory-Servern

CA IAM CS kann so konfiguriert werden, dass Benutzer mit Active Directory-Server (ADS) lokale Identitätsinformationen mit Cloud-basierten Endpunktinformationen synchronisieren können. Sie können zum Beispiel Ihren ADS so einrichten, dass er mit einer Cloud-basierten SalesForce-Installation synchronisiert wird. Ergänzungen oder Änderungen an einer synchronisierten lokalen Benutzergruppe werden dann zur SalesForce-Umgebung übertragen.

Diese Funktion benötigt CA IAM CS, einen unterstützten Endpunkt und den entsprechenden Connector.

Beachten Sie zur Active Directory-Synchronisierungsfunktion Folgendes:

- Diese Funktion unterstützt nur Active Directory. Andere LDAP-Verzeichnisse werden in dieser Version nicht für die Verwendung mit dieser Funktion unterstützt.
- Diese Funktion unterstützt nur Cloud-basierte Endpunkte, für die ein Connector vorhanden ist. In dieser Version zählen Google Apps und SalesForce zu den unterstützten Anwendungen.

Weitere Informationen zu dieser Funktion finden Sie im *Connectors Guide*.

Auditing von Anmelde- und Abmeldeereignissen

Um die Überwachung des Benutzerzugriffs in der CA IdentityMinder-Umgebung zu verbessern, können Sie CA IdentityMinder so konfigurieren, dass die Anmelde- und Abmeldeereignisse in einer Umgebung überwacht werden. Sie können diese protokollierten Ereignisse im Standardbericht "Auditdetails" anzeigen.

Hinweis: Benutzeranmelde- und Benutzerabmeldeereignisse können nicht für CA SiteMinder protokolliert werden.

Sie können diese Einstellungen in der Auditeinstellungsdatei konfigurieren. Weitere Informationen zum Konfigurieren von Anmelde- und Abmeldeereignissen finden Sie im Kapitel "Auditing" des *Konfigurationshandbuchs*.

SHA-2

SHA-2-SSL-Zertifikat-Hashing ist ein kryptografischer Algorithmus, der vom National Institute of Standards and Technology (NIST) und der National Security Agency (NSA) entwickelt wurde. SHA-2-Zertifikate sind sicherer als alle vorherigen Algorithmen. In CA IdentityMinder können Sie SHA-2-signierte SSL-Zertifikate anstelle von Zertifikaten konfigurieren, die mit der SHA-1-Hash-Funktion signiert wurden.

Kapitel 2: Hinweise zur Installation

Dieses Kapitel enthält folgende Themen:

Unterstützte Plattformen und Versionen (siehe Seite 23)
Veraltete und verworfene Komponenten (siehe Seite 23)
JDK-Anforderung für Linux-Installationen (siehe Seite 24)
Nicht verschlüsselte Kennwörter (siehe Seite 24)
Oracle Oracle 11g R2 RAC als Benutzerspeicher und Objektspeicher (siehe Seite 24)
ADAM 2008 als Benutzerspeicher (siehe Seite 24)
Nicht-ASCII-Zeichen verursacht Installationsfehler auf nicht englischsprachigen Systemen (siehe Seite 25)
Installation des Bereitstellungsverzeichnisses auf Linux (siehe Seite 25)
Identity Manager-EAR wird nicht automatisch mit WebLogic bereitgestellt (siehe Seite 26)
Umgehen der Firewall unter Windows 2008 SP2 (siehe Seite 26)
Bereitstellen von JSP-Seiten für Administratoraktionen (siehe Seite 26)
CA IdentityMinder auf Linux 64-Bit mit SiteMinder-Konnektivitätsfehlern (siehe Seite 27)
Verbessern der Leistung bei WebSphere und AIX (siehe Seite 28)
Ignorieren von WebSphere 7/Oracle-Fehlern (siehe Seite 28)

Unterstützte Plattformen und Versionen

In CA CA IdentityMinder r12.6.1 wurden an unterstützten Anwendungsserver-Versionen, -verzeichnissen und -datenbanken Änderungen vorgenommen.

Hinweis: Eine vollständige Liste der unterstützten Plattformen und Versionen finden Sie in der CA Identity Manager-Support-Matrix auf der Website von CA Support.

Veraltete und verworfene Komponenten

Bestimmte Komponenten werden als veraltet markiert, was heißt, dass sie in künftigen Versionen nicht mehr unterstützt werden. Andere Komponenten werden verworfen, was bedeutet, dass sie nicht mehr mit dem Produkt geliefert oder nicht mehr mit dem Produkt getestet werden. Diese Komponenten sind in der CA IdentityMinder Deprecation Policy bei CA Support aufgelistet.

JDK-Anforderung für Linux-Installationen

CA IdentityMinder r12.6.1 benötigt Oracle JDK 1.6.

RedHat 6.x enthält OpenJDK 1.6, was dazu führen kann, dass das CA IdentityMinder-Installationsprogramm hängen bleibt. Stellen Sie sicher, dass Sie die in der CA IdentityMinder-Unterstützungsmatrix angegebene Sun JDK-Version verwenden.

Nicht verschlüsselte Kennwörter

Bei neuen Installationen werden Benutzerkennwörter nicht standardmäßig verschlüsselt. Auch wenn SiteMinder in CA IdentityMinder integriert ist, können Sie die Kennwortverschlüsselung nicht mit "AttributeLevelEncrypt" aktivieren. Dieses Attribut funktioniert nur, wenn SiteMinder nicht installiert ist.

Das Problem wird in einer künftigen Version behoben sein.

Oracle Oracle 11g R2 RAC als Benutzerspeicher und Objektspeicher

Bei Verwendung von Oracle 11g R2 RAC als Benutzerspeicher und Laufzeitspeicher müssen Sie Folgendes ausführen, um die Cluster-Funktionen eines Oracle-Datenbank-Clusters verwenden zu können:

- Verwenden Sie SCAN (Single Client Access Name), um CA IdentityMinder mit Oracle 11g R2 RAC zu installieren.
- Erstellen Sie den Datenbank-*Tablespace* auf der gemeinsam genutzten Festplattengruppe, während ein Tablespace erstellt wird.

ADAM 2008 als Benutzerspeicher

Wenn Sie ADAM 2008 als den CA IdentityMinder-Benutzerspeicher benutzen und Sie CA IdentityMinder mit SiteMinder integrieren, ist SiteMinder r6.0 SP6/r6.x QMR6 erforderlich.

Nicht-ASCII-Zeichen verursacht Installationsfehler auf nicht englischsprachigen Systemen

Während der Installation von CA IdentityMinder extrahiert das Installationsprogramm Dateien in ein Temp-Verzeichnis. Auf einigen lokalisierten Systemen enthält der Standardpfad zum Temp-Verzeichnis Nicht-ASCII-Zeichen. Der Standardpfad zum Temp-Verzeichnis lautet beispielsweise auf spanischen Windows-Systemen:

C:\Documents and Settings\Administrador\Configuración local\Temp

Das Nicht-ASCII-Zeichen sorgt dafür, dass das Installationsprogramm eine leere Übersichtsseite für die Installationsvorbereitungen anzeigt und die Installation anschließend fehlschlägt.

Behelfslösung

Ändern Sie die Tmp-Umgebungsvariable so, dass sie auf einen Ordner verweist, der ausschließlich ASCII-Zeichen enthält.

Installation des Bereitstellungsverzeichnisses auf Linux

Wenn Sie das Bereitstellungsverzeichnis auf einem Linux-System installieren, verwendet das System automatisch IPv6-Adressen, auch wenn Sie beabsichtigen, auf diesem System IPv4 zu verwenden. Alle DSAs scheinen zu funktionieren, jedoch könnte beim Versuch, über Jxplorer eine Verbindung zu den DSAs herzustellen, oder den Bereitstellungsserver zu installieren, die Fehlermeldung "Verbindung abgelehnt" angezeigt werden.

So deaktivieren Sie IPv6 auf Linux

1. Folgen Sie vor der Installation des Bereitstellungsverzeichnisses den Schritten des Red Hat Knowlegde Base-Artikels unter IPv6 auf LINUX deaktivieren.
2. Vergewissern Sie sich, dass die Datei "/etc/hosts" keinen Eintrag für folgende Adresse hat:

   127.0.0.1 *hostname*

Identity Manager-EAR wird nicht automatisch mit WebLogic bereitgestellt

Wenn Sie WebLogic 9 oder 10 im Produktionsmodus einsetzen, wird CA IdentityMinder-EAR möglicherweise nicht automatisch bereitgestellt, wenn Sie den Anwendungsserver nach einer Installation oder einem Upgrade zum ersten Mal starten. Wenn dieser Fall eintritt, stellen Sie "iam_im.ear" manuell aus dem Ordner "user_projects\applications" bereit.

Umgehen der Firewall unter Windows 2008 SP2

In Windows 2008 SP2-Bereitstellungen wird während der Installation die Kommunikation mit CA IdentityMinder-Komponenten wie dem Bereitstellungsserver, dem Java Connector Server und C++-Connector-Server von der Firewall gesperrt.

Fügen Sie Port-Ausnahmen hinzu oder deaktivieren Sie die Windows-Firewall, um in Windows 2008 SP2-Bereitstellungen auf verteilte CA IdentityMinder-Komponenten zuzugreifen.

Bereitstellen von JSP-Seiten für Administratoraktionen

Der CA IdentityMinder-Server umfasst Beispiel-JSP-Seiten für die Ausführung der folgenden Aktionen:

- Anpingen des Anwendungsservers
- Auflisten der bereitgestellten BLTHs
- Auflisten der Information über Objekttypen und Anbieter von verwalteten Objekten
- Auflisten der Plug-in-Informationen
- Ändern der Protokollierungsebenen

Die JSP-Seiten werden an diesem Speicherort installiert:

admin_tools\samples\admin

Der Ordner enthält eine readme.txt-Datei mit Anweisungen für die Verwendung der JSP-Seiten.

Hinweis: Es wird ein Fehler 404 angezeigt, wenn Sie diese JSP-Seiten verwenden, ohne die Anweisungen in der readme.txt-Datei zu befolgen.

CA IdentityMinder auf Linux 64-Bit mit SiteMinder-Konnektivitätsfehlern

Das Installationsprogramm berichtet Fehler bei CA Identity Manager auf Linux 64-Bit, wenn die Option "Verbindung zum SiteMinder herstellen" ausgewählt wurde. Die erforderliche Agentenkonfiguration ist in SiteMinder nicht korrekt

Wichtig! Führen Sie vor der Bereitstellung eines Verzeichnisses oder einer Umgebung die Behelfslösungsschritte durch.

Behelfslösung

1. Rufen Sie den Agentenamen und das Kennwort ab, die Sie bei der Installation angegeben haben. Alternativ können Sie den Wert für die "AgentName"-Eigenschaft folgender Datei entnehmen:

   `\iam_im.ear\policyserver.rar\META-INF\ra.xml`

2. Öffnen Sie die SiteMinder WAM-Benutzeroberfläche und erstellen Sie einen Agenten mit dem Agentennamen. Aktivieren Sie ganz bewusst das Kontrollkästchen "4.x-Agent".

3. Starten Sie den Anwendungsserver und vergewissern Sie sich, dass keine Konnektivitätsprobleme beim Richtlinienserver auftreten.

   Es sollte eine Zeile wie folgende ohne Ausnahmen angezeigt werden:

   ```
   13:40:43,156 WARN [Standard] * Startschritt 2: Versucht, PolicyServerService zu starten
   ```

Verbessern der Leistung bei WebSphere und AIX

Bei einer WebSphere-Installation unter AIX können Sie die Leistung verbessern, indem Sie in der Benutzerkonsole die größtmögliche Heap-Größe festlegen.

Gehen Sie wie folgt vor:

1. Suchen Sie die Datei "server.xml" an folgendem Speicherort:
   `WAS_HOME/profiles/Profile/config/cells/Cell/nodes/Node/servers/Server`
2. Fügen Sie im "jvmEntries"-Element Folgendes hinzu: maximumHeapSize="1000".

   Sie können bei Bedarf auch einen höheren Wert verwenden. Um zum Beispiel maximumHeapSize auf 2 GB (2.048 MB) einzustellen, fügen Sie es so hinzu, wie im folgenden Auszug aus dieser Datei fett angezeigt:

```
<jvmEntries xmi:id="JavaVirtualMachine_1183122130078"
verboseModeClass="false"
   verboseModeGarbageCollection="false" maximumHeapSize="2048"
verboseModeJNI="false" runHProf="false" hprofArguments="
debugMode="false"
debugArgs="-agentlib:jdwp=transport=dt_socket,server=y,suspend=
n,address=7777" genericJvmArguments="">
      <systemProperties xmi:id="Property_1"
name="com.ibm.security.jgss.debug" value="off"
required="false"/>
      <systemProperties xmi:id="Property_2"
name="com.ibm.security.krb5.Krb5Debug" value="off"
required="false"/>
    </jvmEntries>
```

Ignorieren von WebSphere 7/Oracle-Fehlern

Wenn CA IdentityMinder mithilfe eines Oracle-Laufzeitspeichers und der WebSphere 7 Standard JRE installiert wird, wird in den CA IdentityMinder-Protokollen folgender Fehler angezeigt.

> Oracle does not support the use of version 10 of their JDBC driver with the version of the Java runtime environment that is used by the application server.

Dieser Fehler kann ignoriert werden.

Kapitel 3: Upgrades

Folgende Probleme hängen in CA IdentityMinder r12.5 SP1 mit Upgrades zusammen.

Dieses Kapitel enthält folgende Themen:

Unterstützte Upgrade-Pfade (siehe Seite 29)
Neue Active Directory-Rollendefinitionsdatei (siehe Seite 30)
Aktualisieren auf die Datei "jboss.xml" (siehe Seite 30)
64-Bit-Anwendungsserver (siehe Seite 31)
Problem beim Upgrade eines Clusters von CA IdentityMinder r12 CR6 oder einer späteren Version (siehe Seite 31)
Upgrade von r12.5 SP6 oder älter auf WebLogic (siehe Seite 32)
Fehler bei der Umgebungsmigration (siehe Seite 33)
Upgrade-Fehler von Credential Provider (siehe Seite 33)
Interner Fehler des Vista Credential Providers (siehe Seite 33)
Kein Suchfenster mit der Aufgabe "Durchsuchen und Korrelieren" (siehe Seite 34)
Nicht schwerwiegender Fehler nach dem Upgrade des Bereitstellungsmanagers von r12 (siehe Seite 34)
Umbenennen von ACF2-, RACF- und TSS-Endpunkten vor dem Upgrade (siehe Seite 35)

Unterstützte Upgrade-Pfade

Sie können ein Upgrade von folgenden Versionen auf CA IdentityMinder r12.6.1 durchführen:

- CA Identity Manager r12
- CA Identity Manager r12.5
- CA Identity Manager r12.5 SPx
- CA IdentityMinder r12.6

Wenn Sie CA Identity Manager mit einer Version älter als r12 haben, müssen Sie zuerst ein Upgrade auf r12, r12.5 oder r12.5 SP1 bis SP6 durchführen. Diese Versionen enthalten das Imsconfig-Tool, das erforderlich ist, um ein Upgrade mit einer Version älter als r12 durchführen zu können. Danach können Sie das Upgrade auf CA IdentityMinder r12.6.1 durchführen.

Neue Active Directory-Rollendefinitionsdatei

Stellen Sie sicher, dass Sie die neue Rollendefinitionsdatei für Active Directory in jede Umgebung importieren. Die aktuelle CA IdentityMinder-Umgebung kann eine frühere Version der Active Directory-Rollendefinitionsdatei haben. Importieren Sie in diesem Fall die Datei, um ein Upgrade der Rollendefinitionen auf 1.08 durchzuführen. Weitere Details zum Importieren von Rollendefinitionsdateien finden Sie in den im *Upgrade-Handbuch* beschriebenen Verfahren.

Aktualisieren auf die Datei "jboss.xml"

Während eines JBoss-Neustarts oder bei der Initialisierung von CA IdentityMinder werden zahlreiche Fehlermeldungen in der CA IdentityMinder-Datei "server.log" protokolliert. Diese Meldungen beziehen sich auf von JMX verwaltete Ereignisse, aber der empfangende Message Bean ist noch nicht initialisiert. Um dieses Problem zu beheben, enthält die folgende Datei jetzt eine Abhängigkeitsklausel:

```
iam_im.ear\iam_im_identityminder_ejb.jar\META-INF\jboss.xml
```

Die Abhängigkeitsklausel ist in diesem Abschnitt enthalten:

```
<message-driven>
<ejb-name>SubscriberMessageEJB</ejb-name>
<destination-jndi-name>queue/iam/im/jms/queue/com.netegrity.ims.msg.queue
</destination-jndi-name>
<depends>jboss.web.deployment:war=/iam/im</depends>
</message-driven>
```

Stellen Sie sicher, dass dieser Abschnitt in Ihrer "jboss.xml"-Datei enthalten ist. Das Ergebnis ist, dass die empfangende Message Bean initialisiert wird, bevor JMX beginnt, die Ereigniswarteschlange zu verarbeiten.

64-Bit-Anwendungsserver

CA IdentityMinder r12.6.1 unterstützt 64-Bit-Anwendungsserver, die eine bessere Leistung als 32-Bit-Anwendungsserver bieten. Die folgenden Versionen von 64-Bit-Anwendungsservern werden unterstützt:

- JBoss 5.0 und 5.1 Enterprise Application Platform (EAP)
- JBoss 5.1 Open Source
- Oracle WebLogic 11g (10.3.5)
- IBM WebSphere 7.0

Wenn CA Identity Manager gegenwärtig auf der 64-Bit-Version eines dieser Anwendungsserver ausgeführt wird, können Sie ein Upgrade auf CA IdentityMinder r12.6.1 durchführen, indem Sie das im *Upgrade-Handbuch* beschriebene Verfahren befolgen.

Wenn CA Identity Manager gegenwärtig auf einer niedrigeren Anwendungsserverversion oder auf der 32-Bit-Version des Anwendungsservers ausgeführt wird, deinstallieren Sie CA Identity Manager und installieren Sie CA IdentityMinder auf dem neuen Anwendungsserver. Dieser Prozess wird Migration genannt.

Umfassende Details zu Upgrade und Migration finden Sie im *Upgrade-Handbuch*.

Problem beim Upgrade eines Clusters von CA IdentityMinder r12 CR6 oder einer späteren Version

Wenn Sie ein Upgrade an einem Cluster von CA IdentityMinder r12 CR6 oder einer späteren Version auf CA IdentityMinder r12.5 SP1 vornehmen, schlägt das Upgrade möglicherweise fehl, da manche Cluster-Eigenschaften in der Installationsdatei gelöscht wurden.

Behelfslösung

Stellen Sie vor dem Upgrade sicher, dass folgende Eigenschaften in der Datei "im-installer.properties" vorhanden sind:

- WebSphere: Überprüfen Sie, ob der Cluster-Name in DEFAULT_WAS_CLUSTER angegeben ist. Wenn dies nicht der Fall ist, geben Sie ihn manuell ein.
- WebLogic: Überprüfen Sie, ob der Cluster-Name in DEFAULT_BEA_CLUSTER angegeben ist. Wenn dies nicht der Fall ist, geben Sie ihn manuell ein.

Hinweis: Dieses Problem betrifft kein JBoss-Cluster.

Standardmäßig befindet sich die Installationsdatei an folgenden Speicherorten:

- Windows: C:\Program Files\CA\CA Identity Manager\install_config_info\im-installer.properties
- Unix: /opt/CA/CA_Identity_Manager/install_config_info/im-installer.properties

Upgrade von r12.5 SP6 oder älter auf WebLogic

Symptom:

Wenn Sie auf dem WebLogic-Anwendungsserver ein Upgrade von r12.5 SP6 oder älter durchführen möchten, sehen Sie diesen Fehler beim Workflow-Start:

```
WARN  [ims.default] * Startup Step 25 : Attempting to start SchedulerService
ERROR [ims.bootstrap.Main] The IAM FW Startup was not successful
ERROR [ims.bootstrap.Main] org.quartz.SchedulerException: JobStore class
'org.quartz.impl.jdbcjobstore.JobStoreCMT' props could not be configured.
[See nested exception: java.lang.NoSuchMethodException: No setter for
property 'lockHandler.class']
```

Lösung:

1. Halten Sie WebLogic an.
2. Gehen Sie zum Ordner "<IAM-EAR>/APP-INF/lib".
3. Entfernen Sie die folgenden Dateien:
   - common-pool-1.3.jar
   - annotations.jar
   - eurekifyclient.jar
   - quartz-all-1.5.2.jar
4. Starten Sie den Anwendungsserver.
5. Der Workflow-Startfehler wird nicht mehr angezeigt.

Fehler bei der Umgebungsmigration

Symptom:

Wenn Sie ein Upgrade von CA IdentityMinder r12 CR1, CR2 oder CR3 vornehmen, kann beim Importieren Ihrer Umgebungen folgender Fehler auftreten:

Das Attribut "accumulateroleeventsenabled" darf nicht im Element "Provisionierung" auftreten.

Lösung:

Öffnen Sie die Datei "envsettings.xml" im exportierten Env.zip und aktualisieren Sie "accumulateroleeventsenabled" auf "acumulateroleeventsenabled" (entfernen Sie das zweite 'c' in 'accumulate').

Upgrade-Fehler von Credential Provider

Nachdem Sie ein Upgrade des Credential Providers für CA IdentityMinder r12 auf einer 32-Bit-Windows-Plattform durchgeführt haben, ist das Kontrollkästchen "Anmeldeinformationsanbieter für das Kennwort deaktivieren" in der CAIMCredProvConfig-Anwendung deaktiviert.

Behelfslösung

Öffnen Sie die CAIMCredProvConfig-Anwendung, und aktivieren Sie das Kontrollkästchen.

Interner Fehler des Vista Credential Providers

Symptom:

Beim Upgrade von CA IdentityMinder Vista Credential Provider auf 64-Bit-Windows-Plattformen wird die Fehlermeldung *Interner Fehler 2324.2* angezeigt.

Lösung:

Es ist keine Aktion erforderlich, da der Aktualisierungsvorgang erfolgreich abgeschlossen wurde.

Kein Suchfenster mit der Aufgabe "Durchsuchen und Korrelieren"

Wenn Sie CA IdentityMinder r12 *oder* CA IdentityMinder r12.5 aktualisiert haben *und* die Aufgabe "Durchsuchen und Korrelieren" in das neue Wiederholungsmodell migriert haben, funktioniert die Schaltfläche "Durchsuchen" der Aufgabe "Durchsuchen und Korrelieren" nicht richtig.

Behelfslösung

Konfigurieren Sie ein Suchfenster für die Aufgabe, damit die neue "Durchsuchen"-Schaltfläche ein Suchfenster anzeigt, wenn man auf sie klickt.

Nicht schwerwiegender Fehler nach dem Upgrade des Bereitstellungsmanagers von r12

Symptom:

Nachdem Upgrade des Bereitstellungsmanagers von CA IdentityMinder r12 CRx zeigt das Installationsprogramm etwa folgende Meldung an:

```
Der Installationsassistent hat das Upgrade von CA Identity Manager
beendet, aber während des Upgrades traten nicht schwerwiegende Fehler
oder Warnungen auf. Details finden Sie im Installationsprotokoll unter
C:\Programme\CA\CA Identity Manager.
Warnungen/Fehler wurden in Bezug auf die folgenden Komponenten
berichtet
```

Das CA IdentityMinder-Installationsprotokoll enthält den folgenden Eintrag:

```
Install, com.installshield.product.actions.Files, err,
ServiceException: (error code = -30016; message = "Der Prozess kann
nicht auf die Datei zugreifen, weil sie von einem anderen Prozess
verwendet wird."
```

Lösung:

Der Fehler tritt auf, weil das Installationsprogramm kein Verzeichnis erstellen kann, das bereits vorhanden ist. Trotzdem wurde die Installation erfolgreich abgeschlossen, und der Bereitstellungsmanager funktioniert.

Umbenennen von ACF2-, RACF- und TSS-Endpunkten vor dem Upgrade

Leerzeichen in Endpunktnamen werden nicht mehr unterstützt. Wenn Sie Endpunkte mit Leerzeichen im Namen in einer früheren Version erstellt haben, entfernen Sie diese Leerzeichen, bevor Sie das Upgrade auf 12.6 durchführen.

Kapitel 4: Bekannte Probleme

Dieses Kapitel enthält folgende Themen:

Allgemein (siehe Seite 37)
Berichterstellung (siehe Seite 47)
Allgemein (siehe Seite 48)
CA IAM CS und Connector Xpress (siehe Seite 50)
Endpunkttypen (siehe Seite 50)

Allgemein

Folgende Probleme sind allgemein bekannt in CA IdentityMinder r12.5 SP1.

Bereitstellungsverzeichnis lässt sich nicht über die Management-Konsole erstellen

Beim Erstellen eines Bereitstellungsverzeichnisses über die Management-Konsole darf der Domänenname des Bereitstellungsservers keine fremdsprachigen Zeichen enthalten. Folgende Fehlermeldung wird angezeigt:

"could not connect to the LDAP server machinename:20389 with userDN etGlobalUserName=admin,eTGlobalUserContainerName:GlobalUsers,eTNamespacename=CommonObjects,dc=foreignChars, dc=eta and specified password."

AttributeLevelEncryption für Benutzerkennwörter

Wenn Sie die "AttributeLevelEncryption"-Datenklassifizierung für Attribute in der Verzeichniskonfigurationsdatei ("directory.xml") angeben, verschlüsselt CA IdentityMinder den Attributwert im Benutzerspeicher. In der Benutzerkonsole wird der Wert in Klartext angezeigt.

Die folgende Attributbeschreibung zeigt die "AttributeLevelEncryption"-Datenklassifizierung:

```
<ImsManagedObjectAttr physicalname="title" description="Title"
displayname="Title" valuetype="String" maxlength="0"
searchable="false">

<DataClassification name="AttributeLevelEncrypt"/>

</ImsManagedObjectAttr>
```

In Umgebungen mit der folgenden Konfiguration werden bei Verschlüsselung der Kennwörter auf Attributebene Benutzer daran gehindert sich anzumelden:

- CA IdentityMinder-Integration von CA SiteMinder und
- Benutzerspeicher ist eine relationale Datenbank

In dieser Version wurde die "AttributeLevelEncryption"-Datenklassifizierung aus dem Kennwortattribut der folgenden Verzeichniskonfigurationsdateien ("directory.xml") entfernt:

- DirectoryTemplates/RelationalDatabase.xml
- fwSampleRDB.xml
- Samples/NeteAutoRDB/NoOrganization.xml
- Samples/NeteAutoRDB/Organization.xml

Diese Dateien befinden sich im Verzeichnis *admin_tools*.

Hinweis: Weitere Informationen zur Verwaltung vertraulicher Attribute finden Sie im *Konfigurationshandbuch*.

Spezifizieren von LDAP-DN bei Verwendung von TEWS

Symptom:

Bei der Verwendung von TEWS zum Aufrufen der Aufgabe "CreateOracleServerAccountTemplate" können Sie folgende Fehlermeldung zurückerhalten:

```
Error Message: <code>500</code>

<description>Failed to execute CreateOracleServerAccountTemplate. ERROR

MESSAGE: com.ca.iam.model.IAMParseException: Not a valid IAM handle:

'UHGUSERS' ProcessStep::Unknown TabName: null ERRORLEVEL::Fatal</description>
```

Das Problem besteht darin, dass TEWS nicht denselben DN erwartet, der im Bereitstellungsverzeichnis gespeichert ist.

Dieses Beispiel funktionierte nicht:

```
eTORADirectoryName=WSDLOracle4,eTNamespaceName=Oracle Server,dc=im,dc=eta
```

Dieses Beispiel ist der DN, der funktioniert hat:

```
EndPoint=WSDLOracle4,Namespace=Oracle Server,Domain=im,Server=Server
```

Lösung:

Um die Zuordnung zu finden, müssen Sie sich vergewissern, dass die Protokollebenen des Anwendungsservers auf "verbose" festgelegt sind. Führen Sie die Identity Manager-Aufgaben aus, für die Sie die Daten/Pfade benötigen. Die Pfade werden in der Protokolldatei sein. Die Suche mit "<" und "Einfügung in IM_" kann hilfreich dafür sein, die Pfade und auch die Attributwerte zu finden, die von den Aufgaben übergeben werden.

Fehler mit "setpasswd" bei 64-Bit-Linux-Systemen

Symptom:

Auf Linux 64-Bit- und Solaris-Systemen führt "setpasswd" zu folgendem Fehler:
`"/opt/CA/SharedComponents/csutils/bin/expect: error while loading shared libraries: libtcl8.4.so: cannot open shared object file: No such file or directory"`

Lösung:

Legen Sie für LD_LIBRARY_PATH folgenden Wert fest:

/opt/CA/SharedComponents/csutils/lib/tcl8.4

Danach generiert "setpasswd" nicht mehr diesen Fehler.

Problem mit Kennwortrichtlinien bei Verwendung eines kombinierten Benutzerspeicher- und Bereitstellungsverzeichnisses

Symptom:

CA IdentityMinder wendet bestimmte Kennwortrichtlinien nicht bei Bereitstellungen an, die ein kombiniertes Benutzerspeicher- und Bereitstellungsverzeichnis verwenden. Dieses Problem tritt mit Kennwortrichtlinien auf, die die folgenden Regeln und Einschränkungen enthalten:

- Ablauf des Kennworts:
  - Fehlgeschlagene oder erfolgreiche Anmeldeversuche verfolgen
  - Anmeldung authentifizieren
  - Das Kennwort läuft ab, wenn es nicht geändert wird
  - Kennwort-Inaktivität
  - Ungültiges Kennwort
  - Mehrere reguläre Ausdrücke
- Beschränkungen für Kennwort:
  - Mindestanzahl von Tagen vor Wiederverwendung
  - Mindestanzahl von Kennwörtern vor Wiederverwendung
  - Prozentualer Unterschied zum letzten Kennwort
  - Bei der Prüfung auf Unterschiede Sequenz ignorieren

Dieses Problem tritt auf, weil %PASSWORD_DATA% standardmäßig einem binären Attribut anstelle eines Zeichenfolgenattributs zugeordnet wird.

Lösung:

Ordnen Sie in der Management-Konsole %PASSWORD_DATA% einem "eTCustomField"-Attribut zu, das keinem anderen Attribut zugeordnet ist. Zum Beispiel eTCustomField99.

Nachdem Sie die Zuordnung aktualisiert haben, starten Sie die Umgebung neu.

Hinweis: Weitere Informationen zum Aktualisieren eines vorhandenen CA IdentityMinder-Verzeichnisses finden Sie im *Konfigurationshandbuch*.

Verbindung zum CA IdentityMinder-Server kann nicht hergestellt werden, wenn der Kennwortsynchronisierungs-Agent für 64-Bit-Active Directory konfiguriert wird

Symptom:

Wenn der 64-Bit-Kennwortsynchronisierungs-Agent konfiguriert ist, kann ich keine Verbindung zum CA IdentityMinder-Server herstellen, um die Liste der verfügbaren Active Directory-Endpunkte abzurufen.

Lösung:

Sie können nur die Chiffren konfigurieren, die CA IAM CS verwendet. Fügen Sie die drei neuen SSL-FIPS-Chiffren der Chiffrensammlung hinzu, die CA IAM CS verwendet.

Gehen Sie wie folgt vor:

1. Öffnen Sie die folgende Konfigurationsdatei in einem Texteditor:

   ```
   cs_home\jcs\conf\server_osgi_shared.xml
   ```

2. Suchen Sie die Eigenschaft "defaultCipherSuite" in der Datei. Der folgende Beispielcode in der Datei:

   ```
   <property
   name="defaultCipherSuite"><value>FIPS_TLS_PLUS_SSL_Ciphers</value></property>
   <property name="cipherSuites">
               <map>
                   <entry key="FIPS_TLS_PLUS_SSL_Ciphers">
                       <list>
                           <value>TLS_RSA_WITH_AES_128_CBC_SHA</value>
                           <value>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</value>
                           <value>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</value>
                         </list>
   ```

   In diesem Beispiel ist *FIPS_TLS_PLUS_SSL_Ciphers* die Standard-Suite, die der Liste von Chiffren unter der Eigenschaft "cipherSuites" entspricht.

3. Fügen Sie folgende Eingaben der Liste hinzu:

   ```
   <value>SSL_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</value>
   ```

4. Klicken Sie auf "Speichern".

5. Starten Sie den CA IAM CS-Dienst neu.

   Der Kennwortsynchronisierungs-Agent für 64-Bit-Active Directory kann nun ohne Fehler verbunden werden.

Workflow-Teilnehmer-Resolver schlägt für EnableUserEventRoles fehl

Symptom:

Wenn Sie versuchen, Workflow-Einstellungen für die Aufgabe zu ändern, wird folgende Meldung angezeigt:
`Die Option "Primäres Objekt dieser Aufgabe" kann nicht im Abschnitt {0} 'Auflösung - Beschreibung' für die Mehrfachauswahl-Aufgaben festgelegt werden.`

Lösung:

Gehen Sie zur Workflowseite, und ändern Sie den Genehmiger in "Diesem Ereignis zugeordnetes Objekt".

Doppelter Name in "Gesendete Aufgaben anzeigen"

Symptom:

In einigen Hochverfügbarkeitsumgebungen mit hohen Lasten kann der CA IdentityMinder-Server dem Bereitstellungsserver gleichzeitige Anfragen senden und Wettlaufsituationen im Bereitstellungsserver einführen, wenn parallele Änderungsanforderungen an denselben globalen Benutzer verarbeitet werden.

Lösung:

Ändern Sie die folgende Bereitstellungsmanager-Einstellung in "Nein", und starten Sie den Bereitstellungsserver neu.
`Identity Manager-Server/Gleichzeitige Änderung am gleichen globalen Benutzer zulassen`

Hinweis: Wenn es eine Option zum Beenden des Programms beim Zugriff auf globale Benutzer gibt, lassen Sie diese Parametereinstellung auf "Ja".

Fehlermeldung "Nicht gefunden" beim Erstellen einer neuen Umgebung in manchen Bereitstellungen

Wenn CA IdentityMinder mit CA SiteMinder 6.0.5 CR 31 oder späteren Versionen integriert wird, wird möglicherweise die Fehlermeldung "Fehler 404 - Nicht gefunden" angezeigt, wenn Benutzer versuchen, nach einer neuen Umgebungs-URL zu suchen.

Dieses Problem besteht aufgrund eines Zwischenspeicher-Problems im Richtlinienserver.

Behelfslösung

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

Windows:

1. Geben Sie wie folgt ein Kennwort in die SiteMinder-Registrierung ein:
   a. Navigieren Sie zu \\HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\ObjectStore
   b. Fügen Sie den "ServerCmdMsec"-Schlüssel mit folgenden Einstellungen hinzu:
      - Typ: "DWORD"
      - Wert: 1
   c. Starten Sie den Richtlinienserver neu
2. Starten Sie den Anwendungsserver neu.
3. Schließen Sie alle Browser-Instanzen. Verwenden Sie dann eine neue Browser-Instanz, um auf die Umgebungs-URL zuzugreifen.

Solaris:

1. Fügen Sie eine Zeile hinzu zu <CA_HOME folder>/netegrity/siteminder/registry/sm.registry file ServerCmdMsec= 0x1 REG_DWORD
2. Starten Sie den Richtlinienserver neu.
3. Starten Sie den Anwendungsserver neu.
4. Schließen Sie alle Browser-Instanzen. Verwenden Sie dann eine neue Browser-Instanz, um auf die Umgebungs-URL zuzugreifen.

Ändern von zusammengesetzten Attributen mit einzelnem Wert im Identity Manager

Wenn Sie ein zusammengesetztes Attribut mit einzelnem Wert in CA IdentityMinder für einen dynamischen Endpunkt ändern, legen Sie nur einen einzelnen Wert fest. Wenn Sie mehrere Werte festlegen, wird der bestehende Wert gelöscht und das Attribut verfügt über keinen Wert. Dieses Problem tritt im Bereitstellungs-Manager nicht auf.

Beschränkungen des Massendatenladers auf Beziehungsattribut-Ebene

Der Massendatenlader kann die Aufgabenvorgänge auf den Benutzerobjekten nicht auf der Beziehungsattributebene aktualisieren.

- Beziehungsattribute, die nicht vom Massendatenlader aktualisiert werden, sind Benutzerzugriffsrollen, Benutzer-Admin-Rollen, Benutzer-Bereitstellungsrollen, Benutzergruppenmitgliedschaft und Gruppen.
- Beziehungsattribute, die überschrieben werden würden, wenn Sie alte Attributwerte durch neue Attributwerte aus der Massendatenladerdatei ersetzen, sind Gruppen-Administratoren und benutzerdefinierte oder Standard-Attribute mit mehreren Werten.

Fehler beim Erstellen einer bereitstellungsaktivierten Umgebung mithilfe von Token-Vorlagen

In diesem Fall kann CA IdentityMinder die Rolle des Bereitstellungs-Synchronisations-Managers nicht dem im Umgebungserstellungsassistenten definierten eingehenden Administrator zuweisen.

Wenn die Umgebungsvorlage Token oder übersetzte Zeichenfolgen für den Rollennamen des Bereitstellungs-Synchronisations-Managers hat, schlägt die Suche fehl und der NoSuchObjectException-Fehler wird ausgelöst.

Voraussetzungen für Oracle-Anwendungen

Sie müssen NLS_LANG als eine Systemumgebungsvariable mit dem Wert .UTF8 festlegen.

Hinweis: Der Punkt (.) muss vor UTF8 auf dem System stehen, wo der Connector-Server installiert wird.

Oracle 11gR2 RAC-Benutzerspeicher: Groß- und Kleinschreibung bei der Suche

Symptom:

Wenn Oracle 11gR2 RAC der Benutzerspeicher ist, ergibt die Suche nach Benutzern, Gruppen oder Organisationen manchmal bietet keine Ergebnisse, obwohl die Objekte vorhanden sind.

Lösung:

Für diesen Benutzerspeicher muss bei der Suche die Groß-/Kleinschreibung beachtet werden. Zum Beispiel liefert die Suche nach *Schmidt* keine Ergebnisse, wenn der Benutzer als *SCHMIDT* in der Datenbank erstellt wurde. Verwenden Sie die gleiche Schreibweise, mit der das Objekt in der Datenbank erstellt wurde.

CA IdentityMinder unter JBoss nimmt Verbindung zu Oracle nicht wieder auf

Symptom:

Bei Verwendung von JBoss 5.x mit der Datenquelle einer Oracle-Datenbank und beim Upgraden von CA IdentityMinder auf Version r12.5 fällt beim Neustart des Datenbankservers die Anwendung aus. Der Ausfall wird verursacht, weil JBoss die Eigenschaft "background-validation-minutes" durch "background-validation-millis" ersetzt.

Lösung:

Gehen Sie folgendermaßen vor, um dieses Problem zu beheben:

1. Halten Sie den Anwendungsserver an.
2. Öffnen Sie die Datenquellendateien unter */JBoss-Ordner/Server/Standard [oder Servername in Cluster]/deploy* , und löschen Sie die folgende Zeile:

   <background-validation-minutes> </background-validation-minutes>
3. Fügen Sie folgende Zeile hinzu:

   <background-validation-millis>120000</background-validation-millis>

   Hinweis: 120000 ist das Äquivalent zu 2 Minuten, die früher standardmäßig für "background-validation-minutes" angegeben wurden. Konfigurieren Sie den Wert entsprechend den Geschäftsanforderungen.
4. Starten Sie den Anwendungsserver neu.

Hinweis: Das Problem hat keine Auswirkungen auf die neue Installation von CA IdentityMinder.

Fehler bei "Zum Hauptinhalt wechseln" in Mozilla Firefox

Symptom:

Oben in der Benutzerkonsole sehen Sie den Link "Zum Hauptinhalt wechseln". Dieser Link verschiebt den Hauptrahmen der Seite an das obere Ende. Allerdings schlägt dieser Link in Mozilla Firefox fehl.

Lösung:

Verwenden Sie Microsoft Internet Explorer 8 oder höher mit JAWS, um diese Funktion zu unterstützen.

Fehler bei gleichzeitigen Änderungen an einem Benutzer

Die Aufgabe "Benutzer ändern" schlägt in folgenden Situationen fehl:

- Wenn Sie versuchen, einen Benutzer zu deaktivieren, während Sie diesen Benutzer ändern, schlägt die Aufgabe fehl.
- Wenn Sie das Attribut "forcePasswordChange" dem Fenster "Benutzerprofil" hinzufügen, während Sie einen Benutzer ändern, schlägt die Aufgabe fehl.

Änderung an Policy Xpress-Syntax

Symptom:

Aufgrund einer Änderung an der Policy Xpress-Syntax kann ein Fehler auftreten. Der Fehler tritt auf, wenn die Richtlinie die Zeichenfolgenanalyse für die Konto-ID verwendet und der Benutzer mehrere Konten auf einem flachen Endpunkt hat. Endpunkte wie Oracle, OS400 und Microsoft SQL haben Konten als virtuelle Container, die sich unter dem Endpunktnamen befinden. Beim Starten unter 12.6.1 ist die Syntax der Konto-ID folgendermaßen:

- Für flache Connectors, EndpointName: EndpointName:AccountName
- Für hierarchische Connectors, EndpointName:AccountContainerPath:AccountName

Lösung:

Suchen Sie die Policy Xpress-Richtlinien, die die Zeichenfolgenanalyse für die Konto-ID verwenden. Aktualisieren Sie diese Richtlinien entsprechend der neuen Syntax.

Aktualisieren gemäß SAP-Hilfethema

Die Hilfe für die auf SAP r3-Konten bezogene Standardsregisterkarte sollte diese Definition für die Dezimale Notation haben.

- Gibt die unterschiedlichen Dezimalschreibweisen an.
- Folgende Optionen stehen zur Auswahl:

  1.234.567,89

  1,234,567.89

  1 234567,89

Berichterstellung

Folgende Probleme hängen in CA IdentityMinder r12.5 SP1 mit der Berichterstellung zusammen.

Bei der Benutzerfiltersuche ist in den Benutzerkonten und den XML-Dateien zu benutzerdefinierten Snapshots der Endpunktkonten die Groß-/Kleinschreibung zu beachten.

Symptom:

Beim Erstellen eines Filters auf %USER_ID% in den *useraccounts*-Exportelementen in *Benutzerkonten* und den XML-Dateien zu benutzerdefinierten Snapshots der *Endpunktkonten* zeigt der Bericht die Ergebnisse nicht an, obwohl der Benutzer vorhanden ist.

Lösung:

Bei der Filtersuche muss die Groß-/Kleinschreibung beachtet werden.

Satisfy=All funktioniert in XML-Datei nicht ordnungsgemäß

In einer XML-Datei mit Snapshot-Parametern reagieren die Parameter satisfy=all und satisfy=any beide identisch mit satisfy=any (ähnlich wie ein OR-Operator).

Problem beim Verwenden mehrerer Filter auf Endpunktobjekten

Symptom:

Wenn eine Snapshot-Definition mit Endpunktobjekt mithilfe mehrerer Filter erstellt wird, werden keine Endpunktdaten erfasst.

Lösung:

Auf der Registerkarte "Snapshotrichtlinien" wird anstelle der Auswahl mehrerer Endpunktobjekte das "*"-Sternchen angeben, um mehrere Endpunktobjekte auszuwählen.

Snapshot erfasst keine Gruppenobjektdaten

Symptom:

Wenn eine Snapshot-Definition mit einem Gruppenobjekt und unter Verwendung von "org-filter" erstellt wird, werden keine Gruppendaten erfasst.

Lösung:

Auf der Registerkarte "Snapshotrichtlinien" wird im Drow-down-Menü anstelle der Auswahl von "org-filter" die Option "(alle)" ausgewählt.

Allgemein

Folgende sind allgemeine Bereitstellungsprobleme in CA IdentityMinder r12.5 SP1.

Umbenennen von Bereitstellungsrollen wird nicht unterstützt

Das Umbenennen von Bereitstellungsrollen, nachdem sie erstellt wurden, wird nicht unterstützt.

Solaris ECS-Protokollierung oberhalb der INFO-Ebene kann die Leistung des Bereitstellungsservers verringern

Das Aktivieren der ECS-Protokollierung oberhalb der INFO-Ebene führt dazu, dass Protokolle geschrieben werden, bevor Sie eine Antwort erhalten. Dadurch wird Ihre Anfrage verzögert, während das Protokoll geschrieben wird.

Behelfslösung

Deaktivieren Sie die ECS-Protokollierung, falls Sie feststellen, dass die Leistung des Bereitstellungsservers beeinträchtigt ist.

Fehler "Bereits vorhanden" beim Hinzufügen eines Endpunkts

Wenn Sie einen Endpunkt löschen und mit genau demselben Namen wieder hinzufügen, gibt der Bereitstellungsserver manchmal eine Fehlermeldung aus, dass bereits ein Endpunkt mit dem Namen existiert. Dies kann auftreten, wenn Sie mehrere Connector-Server zum Verwalten des Endpunkts konfiguriert haben. Der Grund für das Fehlschlagen ist ein Problem beim Löschen des Endpunkts, bei dem nicht alle Connector-Server vom Löschen benachrichtigt wurden.

Behelfslösung

Starten Sie alle Connector-Server, die für die Endpunktverwaltung konfiguriert sind, neu.

Fehler bei der Korrelation eines Microsoft SQL-Endpunkts

Symptom:

Die Korrelation eines Microsoft SQL-Endpunkts schlägt mit der folgenden Meldung fehl: `Object MS SQL Logins global users creation failed. Unable to determine object class from distinguished name.`

Dieser Fehler tritt auf, wenn für einen Microsoft SQL-Endpunkt alle Container und nicht nur die Container mit Konten ausgewählt werden.

Lösung:

1. Erstellen Sie eine Definition für "Durchsuchen und Korrelieren", und suchen Sie nach einem Microsoft SQL-Endpunkt.
2. Suchen Sie nach allen Containern, aber wählen Sie nur den *Endpunktnamen* als Container aus.
3. Wählen Sie "Durchsuchen und Korrelieren"-Attribute aus.
4. Führen Sie die Definition "Durchsuchen und Korrelieren" aus.

Einschränkung beim SiteMinder-Anmeldenamen für globalen Benutzernamen

Folgende Zeichen oder Zeichenfolgen darf ein globaler Benutzername nicht enthalten, wenn der Benutzer sich auf dem SiteMinder-Richtlinienserver anmelden können soll:

&
*
:
( )

Behelfslösung

Vermeiden Sie die Verwendung dieser Zeichen im globalen Benutzernamen.

CA IAM CS und Connector Xpress

Die folgenden Probleme beziehen sich auf CA IAM Connector Server (CA IAM CS) und Connector Xpress.

Hinweis: In CA IdentityMinder 12.6 ist Java Connector Server (Java CS oder JCS) in CA IAM Connector Server umbenannt worden (CA IAM CS).

JNDI-Kontoverwaltungsfenster – das Erstellen von Konten mit mehreren strukturierten Objektklassen schlägt fehl

Sie können keine Konten mit mehreren strukturierten Objektklassen erstellen.

Endpunkttypen

Folgende Probleme hängen in CA IdentityMinder r12.5 SP1 mit der Verwaltung von Endpunkttypen zusammen.

Allgemein

Die folgenden Abschnitte beschreiben die für die verschiedenen Connectors bekannten Probleme:

Endpunkte mit automatischer Wiederholungsversuchssperre müssen mit einem großzügigen Limit für Wiederholungsversuche konfiguriert werden.

Für Endpunkte, deren Sperrwert für automatische Wiederholungsversuche bei "N" liegt, sollte das Konto, das zur Verbindung mit dem Endpunkt benutzt wird, der Java CS verwendet, so konfiguriert sein, dass es einen großzügigen (oder unbegrenzten) Wert "N" besitzt, da die Zahl der Verbindungsversuche vom Java CS schnell erreicht ist.

Wenn das Konto vom System gesperrt wird, weil der "N"-Wert überschritten wurde, kann die Verwendung systemeigener Tools zur Entsperrung des Kontos erforderlich sein, um wieder auf den Endpunkt zugreifen zu können. Dies hängt vom exakten systemeigenen Sperrverhalten des Endpunkts ab.

Fehler in Endpunkt-Suchfenstern nach dem Upgrade von 12.5 SP6 oder älter

Symptom:

Ein Fehler, der der folgenden Meldung ähnelt, tritt auf, wenn Sie Rollendefinitionsdateien von Endpunkt aus r12.5 SP6 oder älter in r12.5 SP7 oder höher importieren:

"Error in screen definition "Default Endpoint Type Primary Group Endpoint Capability Search" with tag "DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch" Error: The type "UNKNOWN" is not a valid object type."

In CA Identity Manager r12.5 SP7 wurden bestimmte Objekte umbenannt. Auf diese Objekte wird in Endpunktfunktions-Suchfenstern verwiesen. Nach dem Upgrade auf r12.5 SP 7 oder höher kann ein Fehler auftreten, wenn Sie Rollendefinitionsdateien importieren, die Fenster einschließen, die sich auf die alten Objektnamen beziehen.

Dieses Problem ist in Active Directory und CA Access Control-Endpunkten identifiziert worden.

Beachten Sie das folgende Beispiel für einen Active Directory-Endpunkt:

In CA Identity Manager r12.5 SP6 bezog sich der Suchfenstername von Active Directory-Endpunkten auf das Objekt ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP.

Der Objektname wird in der folgenden Bildschirmdefinition angezeigt:

```
<Screen name="Default Active Directory Primary Group Endpoint
Capability Search"
tag="DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

Object="ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP">
```

In CA Identity Manager r12.5 SP7 wurde der Objektname in "ACTIVEDIRECTORY_ETADSGROUP" geändert.

Der neue Objektname wird in der folgenden Bildschirmdefinition angezeigt:

```
<Screen name="Default Active Directory Group Endpoint Capability
Search"

tag="DefaultActiveDirectoryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

object="ACTIVEDIRECTORY_ETADSGROUP">
```

Lösung:

Löschen Sie ggf. die Bildschirmdefinitionen, die sich auf den alten Objektnamen beziehen, bevor Sie eine Rollendefinitionsdatei importieren.

Kontovorlagen sind in der Benutzerkonsole auf einem "Erstellen"- oder "Verändern"-Task nicht mit Konten synchronisiert.

Symptom:

Die Benutzerkonsole unterstützt keine explizite Kontensynchronisierung.

Lösung:

Verwenden Sie den Bereitstellungs-Manager, um Konten mit Kontovorlagen zu synchronisieren.

Einen Endpunkt direkt zu verändern, verursacht einen Fehler beim Importieren zwischen Endpunkt und Bereitstellungsserver.

Wenn der Endpunkt direkt verändert wird (nicht anhand des Bereitstellungsservers), wird beim Import ein Fehler wegen inkonsistenter Daten zwischen dem Endpunkt und Bereitstellungsserver zurückgegeben. Zwei Beispiele:

- Es wurden unter Verwendung von systemeigenen Tools Tabellen vom MSSQL-Endpunkt entfernt, was dazu führte, dass manche Benutzer nicht mehr vorhandene Ressourcen erhielten.

  Um den Fehler zu beheben, durchsuchen Sie den Endpunkt mit Hilfe des Bereitstellungsservers erneut.

- Es wurden Serverrollen vom Endpunkt gelöscht, und die Kontovorlagen, denen diese Serverrollen noch zugewiesen waren, erhielten zusätzliche Rollen, die auf dem Endpunkt nicht mehr vorhanden sind.

  Um den Fehler zu beheben, entfernen Sie diese "beseitigten" Serverrollen manuell von den Kontovorlagen.

Einschränkung für den Endpunktnamen von ACF2 ACFESAGE-, RACF IRRDBU00- und TSSCFILE-Connectors

Symptom:

Wenn Sie versuchen, einen Endpunkt mit einem Endpunktnamen wie "Benutzer testen", "Benutzer-Test" oder "_Benutzertest" auf Dumpfile-Connectors zu erstellen, wird bei der Endpunkterstellung ein Fehler mit folgender Meldung verursacht: "Cannot create pool able connection factory" (Es konnte keine Pool-fähige Connection Factory erstellt werden).

Lösung:

Leerzeichen sind in Endpunktnamen für ACF2 ACFESAGE-, TSSCFILE- oder RACF-IRRDBU00-Connectors nicht mehr erlaubt. Der Endpunktname für diese Connectors hat auch die folgenden Einschränkungen:

- Muss zwischen 1 und 30 Zeichen lang sein
- Fängt mit alphanumerischen Zeichen an
- Enthält nur alphanumerische Zeichen und/oder "_"-Zeichen.

Bevor Sie ein Upgrade auf diese Version durchführen, löschen Sie die vorhandenen Mainframe-Dumpfile-Endpunkte, deren Namen nicht den Einschränkungen entsprechen.

Zugriffssteuerung

Texte der Schaltflächen des Kalenderfensters sind in Englisch

Wenn Sie im CA Access Control-Endpunkt eine Kontovorlage erstellen, werden im Kalenderfenster unter der Registerkarte "Anmeldung" die Schaltflächen "OK" und "Abbrechen" auf Englisch angezeigt.

Entfernen von Gruppen aus einem Access Control-Konto

Symptom:

Wenn Sie eine systemeigene Gruppe aus einem systemeigenen Benutzerkonto entfernen, das vom Access Control Connector bereitgestellt wurde, werden die systemeigenen Gruppen in einem zweistufigen Prozess entfernt. Der zweistufige Prozess entfernt alle vorhandenen Gruppenmitgliedschaften und fügt dann alle erforderlichen Gruppenmitgliedschaften wieder hinzu. Dies sorgt für die korrekte Gruppenmitgliedschaft des Kontos, kann bei einigen Kunden aber zu betrieblichen Problemen führen.

Lösung:

Wenn Sie den zweistufigen Prozess nicht verwenden möchten, können Sie Connector XPress verwenden, um eine C++ Connector Server (CCE)-Definition zu erstellen. Die CCE-Definition kann direkt mit dem Bereitstellungsserver verbunden werden anstelle eines Routings über CA IAM CS. Diese Umgehungslösung führt zu einer einstufigen Gruppenänderung für ACC-Konten. Allerdings können Sie die Benutzerkonsole nicht verwenden, um ACC-Kontogruppenmitgliedschaften zu verwalten. Um ACC-Kontogruppenmitgliedschaften zu verwalten, verwenden Sie den Bereitstellungsmanager.

Hinweis: Weitere Informationen zur Verwendung von Connector Xpress für die Erstellung einer C++ Connector Server-Definition finden Sie unter "How You Set a Managing Connector Server" (Einrichten eines verwaltenden Connector-Servers) im *Connector Xpress-Handbuch*.

CA Arcot

Schützen von ArcotID-Aufgaben beim Schützen von CA SiteMinder CA IdentityMinder

Wenn CA IdentityMinder von CA SiteMinder mithilfe eines Arcot-Authentifizierungsschemas geschützt wird, funktionieren die folgenden Aufgaben in CA IdentityMinder nicht:

- Meine ArcotID erstellen/zurücksetzen
- Meine ArcotID herunterladen

Die ArcotID-Anmeldeinformationen aktivieren Zwei-Faktor-Authentifizierung für CA SiteMinder-Anwendungen, die von einem Arcot-Authentifizierungsschema geschützt werden.

CA SiteMinder unterstützt nur ein einziges Authentifizierungsschema für eine geschützte Ressource. Alle CA IdentityMinder-geschützten Aufgaben haben die gleiche URL, die von einem CA SiteMinder-Authentifizierungsschema geschützt wird.

Verwenden Sie keine Arcot-Authentifizierung, um die URL für den Zugriff auf CA IdentityMinder-geschützte Aufgaben zu schützen.

Wenn die Arcot-Authentifizierung die URLs von CA IdentityMinder-geschützten Aufgaben schützt, muss Benutzern eine ArcotID für den Zugriff auf Aufgaben wie "Meine ArcotID erstellen/zurücksetzen" oder "Meine ArcotID herunterladen" bereitgestellt werden. Benutzer, die auf diese Aufgaben zugreifen, haben noch kein ArcotID. Sie können diese also nicht bereitstellen, um auf die Aufgaben zugreifen zu können.

Wenn CA IdentityMinder-Aufgaben von CA SiteMinder geschützt werden, verwenden Sie ein anderes Authentifizierungsschema als Arcot, wie Active Directory oder LDAP, um dieses Problem zu verhindern.

Hinweis: Da "Meine ArcotID erstellen/zurücksetzen" oder "Meine ArcotID herunterladen" sensible Aufgaben sind, empfiehlt CA Technologies ausdrücklich, diese Aufgaben als geschützte Aufgaben zu konfigurieren. Wenn Sie diese Aufgaben als öffentliche Aufgaben konfigurieren, können Benutzer auf diese zugreifen, ohne Anmeldeinformationen anzugeben.

Weitere Informationen zu öffentlichen Aufgaben finden Sie unter Self-Service-Aufgaben im "Benutzerkonsolendesign-Handbuch".

Active Directory

Folgende Abschnitte beschreiben die bekannten Probleme für den Active Directory Connector:

Falsche Ergebnisse bei der Suche in einer Unterstruktur mit Active Directory Connector

Bei einer Suche in einer Unterstruktur, die mehrere Organisationseinheiten mit einer großen Anzahl an Objekten in den einzelnen Organisationseinheiten enthält, kann es passieren, dass die Suche fälschlicherweise keine Objekte zurückgibt. Wenn die Suche z. B. auf einen Grenzwert von 500 festgelegt wird und die Anzahl der Objekte in den einzelnen Organisationseinheiten diese Größe überschreitet, werden keine Ergebnisse zurückgegeben. Auch wenn der Suchfilter den Grenzwert für die Suche auf einen Wert unter 500 beschränkt, kann es immer noch vorkommen, dass fälschlicherweise keine Objekte zurückgegeben werden.

Behelfslösung

Erhöhen Sie den Such-Grenzwert.

CA SSO für den Connector des Servers für erweiterte Richtlinien

Folgende Abschnitte beschreiben die bekannten Probleme für den CA SSO Connector des Servers für erweiterte Richtlinien:

PLS-Connector kann nicht mehr als 2000 Konten zu Anwendungen hinzufügen

Es können nicht mehr als 2000 PLS-Konten gleichzeitig zu einer Anwendung hinzugefügt werden. Wenn Sie mehr als 2000 PLS-Konten hinzufügen möchten, müssen Sie die Konten in mehrere Operationen aufteilen.

DB2 und DB2 für z/OS

Folgende Abschnitte beschreiben die bekannten Probleme für die DB2 und DB2 für z/OS Connectors:

Fehler beim Speichern eines Datum-Datentyps aufgrund eines Datentypenkonflikts

Symptom:

Wenn ich das Datumstypattribut auf einem DB2-Endpunkt (JDBC DB2 für IBM i) festlege, wird der folgende Fehler angezeigt:

```
Bad SQL Grammar: Data type mismatch. (YYYY-MM-DD)
```

Lösung:

Bearbeiten Sie die ConnectionURI auf der Endpunktseite des Bereitstellungsmanagers, und fügen Sie *date format=iso* hinzu. Die letzte URI wird wie folgt angezeigt:*jdbc:as400://<host>:CA Portal/<db>;prompt=false;date format=iso;*. Beachten Sie den Abstand zwischen *date* und *format*.

E2Kx

Folgende Abschnitte beschreiben die bekannten Probleme für den E2Kx Connector:

E2K CAFT-Fehler beim Verwalten von Postfachberechtigungen

Möglicherweise wird bei der Verwaltung von Postfachrechten auch dann die Fehlermeldung “CAFT Message : Access denied - or command failed to execute” (CAFT-Meldung: Zugriff verweigert – oder Befehl konnte nicht ausgeführt werden) zurückgegeben, wenn Ihr Exchange Remote Agent korrekt konfiguriert ist.

Dies kann vorkommen, wenn die Liste der Postfachrechte mehrere Berechtigungen für dasselbe Objekt enthält. Normalerweise passiert dies, wenn die verwalteten Austauschobjekte Rechte übergeordneter Objekte übernehmen.

E2K7-Mailbox nach erster Erstellung nicht synchronisiert

Aktivieren Sie die Option "Starke Synchronisierung verwenden", erstellen Sie eine Kontenvorlage und synchronisieren Sie einen globalen Benutzer mit der Kontenvorlage. Klicken Sie danach mit der rechten Maustaste auf den globalen Benutzer und wählen Sie die Option "Kontensynchronisierung" aus. Die Mailbox-Rechte sind nicht synchronisiert.

Behelfslösung

Wählen Sie unter "Exchange Advanced,Mailbox Rights, Add (usingSHIFT+ADD method), 'NT AUTHORITY\Authenticated Users'" nur 'Read permissions' aus.

E-Mail-Adressen nicht in für E-Mails aktivierte Gruppen festgelegt

Sie erstellen eine Gruppe und wählen die Option "Austausch-E-Mail-Adresse erstellen" aus, jedoch ist für die Gruppe keine E-Mail-Adresse festgelegt.

Behelfslösung

Gehen Sie zur Registerkarte "E-Mail-Adressen" und geben Sie dort nach Erstellung der Gruppe die neue E-Mail-Adresse an.

Fehlermeldung wird angezeigt, beim Versuch, ein Konto mit einer E27K-Mailbox zu verändern

Wenn Sie versuchen, ein Konto mit einer E27K-Mailbox zu verändern, wird eine Fehlermeldung angezeigt. Dieser Fehler ist gutartig und kann ignoriert werden.

Fehlermeldung nicht ausreichend beim Versuch, eine E2Kx-Mailbox zu erstellen

Für Zeichen innerhalb des INT-Feldes wird eine ungenügende Fehlermeldung angezeigt. Dieser Fehler, [-]?[\d]*, zeigt an, dass der Wert des angeforderten Feldes eine Zahl sein muss.

Meldungseinschränkungen erlauben nicht, die Optionen 'Nur von' und 'Von allen außer' im Bereitstellungs-Manager gleichzeitig auszuwählen.

Im Exchange Server 2007 können Administratoren sowohl die Option 'In der folgenden Liste nur Meldungen von Sendern akzeptieren' als auch die Option 'In der folgenden Liste Meldungen von Sendern ablehnen' auswählen. Im Bereitstellungs-Manager kann nur eine Option ausgewählt werden. So war die Funktionsweise in Exchange 2003. Wenn in Exchange 2007 beide Optionen systemeigen ausgewählt werden, ist diese Funktion im Bereitstellungs-Manager fehlerhaft.

Google Apps

In den folgenden Abschnitten werden die bekannten Probleme für den Google Apps-Connector beschrieben:

Google-Apps: Fehlermeldung beim Erstellen von Google Apps-Konten

Symptom:

Beim Erstellen eines Google Apps-Kontos erhalte ich die Fehlermeldung *Ausführung von 'Google Apps-Benutzer erstellen' fehlgeschlagen. Google Apps-Benutzer wurde erstellt, jedoch schlug ein zusätzlicher Vorgang fehl*.

Das Konto wird in CA IdentityMinder und auf dem Google Apps-Endpunkt erstellt, aber es ist in der CA IdentityMinder-Benutzerkonsole nicht sichtbar, weil es nicht dem globalen Benutzer zugeordnet ist.

Lösung:

Der Fehler tritt auf, wenn Sie versuchen, ein Konto mit dem gleichen Spitznamen und Benutzernamen zu erstellen.

Um das Problem zu beheben, durchsuchen und korrelieren Sie den Google Apps-Endpunkt

Das Benutzerkonto, das Sie erstellt haben, ist dem globalen Benutzer in CA IdentityMinder zugeordnet und wird nun angezeigt.

Google Apps - Mehrere Google Apps-Endpunkte auf demselben Java CS

Proxy-Einstellungen des Google Apps-Connectors sind systemübergreifende Eigenschaften. Wenn Sie zwei oder mehr Google Apps-Endpunkte auf dem gleichen Java CS erstellen, verwenden Sie den gleichen Proxy-Server, Port, Benutzernamen und Kennwort für alle Google Apps-Endpunkte auf demselben Java CS.

Google Apps - Fehlermeldung "HTTP 403: Verboten" bei Verwendung der NTLM-Authentifizierung

Symptom:

Wenn ich versuche, NTLM-Authentifizierung zu verwenden, erhalte ich den Fehler *HTTP 403: Verboten* vom Proxy-Server, und die Google Apps-Domäne wird nicht aufgerufen.

Lösung:

Der Fehler tritt auf, weil Java CS auf einem Windows-Computer als ein Windows-Dienst installiert wird und standardmäßig als lokales System ausgeführt wird.

Wenn Java CS auf einem Windows-Computer ausgeführt wird und NTLM das stärkste vom HTTP-Proxy unterstützte Authentifizierungsschema ist, versucht der Google Apps-Connector, NTLM-Authentifizierung mit dem HTTP-Proxy zu verwenden.

Wenn Ihr HTTP-Proxy-Server NTLM-Authentifizierung verwendet, konfigurieren Sie Java CS zur Ausführung unter einem Windows-Domänenkonto oder einem lokalen Windows-Konto.

So konfigurieren Sie die NTLM-Authentifizierung

Führen Sie einen der folgenden Schritte aus:

- Führen Sie Java CS mit einem Windows-Konto aus, das mit dem HTTP-Proxy-Server authentifiziert werden kann, ohne einen Benutzernamen und ein Kennwort für Proxyauthentifizierung anzugeben, wenn Sie den Endpunkt erstellen.
- Führen Sie Java CS mit einem Windows-Konto aus, das nicht mit dem HTTP-Proxy-Server authentifiziert werden kann, und geben Sie einen HTTP-Benutzernamen und ein Kennwort an, das mit dem Proxy authentifiziert werden kann, wenn Sie den Endpunkt erstellen.

Hinweis: Wenn Sie einen Windows-Domänenbenutzer für HTTP-Proxyauthentifizierung verwenden, setzen Sie die Windows-Domäne, in der sich der Benutzer befindet, als Präfix vor den HTTP-Proxy-Benutzernamen. Beispiel: "DOMAIN|ProxyBenutzerkontoname".

Kontosuchfehler von Google Apps

Symptom:

Die Suche nach einem Google Apps-Konto auf Basis des Vor- oder Nachnamens schlägt fehl.

Lösung:

Die Aktualisierung auf den Vor- oder Nachnamen eines Benutzers durch Google Apps kann bis zu 30 Minuten dauern. Deswegen schlägt die Suche nach dem neuen Namen in CA IdentityMinder fehl. Warten Sie nach einer Namensänderung 30 Minuten, bevor Sie bei der Suche den neuen Namen verwenden.

PeopleSoft

In den folgenden Abschnitten werden die bekannten Probleme für den PeopleSoft-Connector beschrieben:

Suchen können im Bereitstellungsmanager fehlschlagen

Wenn Sie den Bereitstellungsmanager verwenden, um nach einem PeopleSoft-Endpunkt mit PeopleTools 8.49 zu suchen, gibt die Suche nach PPS-Benutzern für die Zuweisung zu den Feldern "Alternative Benutzer-ID", "ID des überwachenden Benutzers" und "Arbeit neu zuweisen zu" in einigen Fällen keine Ergebnisse zurück.

Es gibt zwei Problemumgehungen für dieses Problem:

- Verwenden Sie die CA IdentityMinder-Benutzerkonsole, um PeopleSoft-Endpunkte zu verwalten (bevorzugt).
- Geben Sie den Wert in die Bereitstellungsmanager-Felder ein, ohne Suchen auszuführen. Der Wert ist immer noch abhängig von der Validierung, sodass die Zuweisung beim Anklicken der Schaltfläche "Übernehmen" fehlschlägt, wenn der eingegebene Wert kein PPS-Benutzer ist.

SAP

Folgende Abschnitte beschreiben die bekannten Probleme für den SAP Connector:

SAP-vertragliche Benutzertypen zuweisen

Wenn ein vertraglicher Benutzertyp einem Benutzer auf der Registerkarte "Lizenzdaten" zugewiesen wird, kann die Änderung nur auf das Master-System und auf kein Tochter-System angewendet werden.

Behelfslösung

Die vertraglichen Lizenztypen für die untergeordneten Elemente können systemabhängig verändert werden.

Der SAP-Endpunkt wurde nicht vorher von der Datei "SAPlogon.ini " aufgefüllt.

Wenn der Bereitstellungs-Manager in Windows 2008 ausgeführt wird, werden die Endpunktdetails für SAP nicht vorher von der Datei "SAPlogon.ini" aufgefüllt.

Hinweis: Dieses Problem ist typisch für den nur auf Windows 2008 ausführbaren Bereitstellungs-Manager.

Behelfslösung

Sie müssen den Inhalt der Datei "SAPlogon.ini" manuell in den Bereitstellungs-Manager eingeben.

Pflichtfelder im SAP-Attribut "Vertraglicher Benutzertyp"

Der vertragliche Benutzertyp, der in der Registerkarte "Lizenzdaten" des Kontos angegeben ist, darf keine anderen Pflichtfelder enthalten als das Feld LIC_TYPE. Wenn Sie z. B. den Namen von einem SAP R3-System (SYSID) angeben sollen, um einen vertraglichen Benutzertyp zu verwenden, wird die Zuweisung fehlschlagen, und Sie erhalten eine Fehlermeldung, dass ein Wert für den Namen des SAP R3-Systems fehlt.

Das vertragliche Benutzertyp-Attribut in der Registerkarte für Kontolizenzdaten funktioniert nicht für alle Lizenztypen.

Wenn ein Benutzertyp aus der verfügbaren Liste ausgewählt wird, funktionieren nur manche Benutzertypen. Manche Lizenztypen verursachen den Funktionsaufruffehler 'BAPI'. Der Grund dafür ist, dass manche Benutzertypen Extrafelder enthalten, die nicht erkannt werden.

Siebel

Folgende Abschnitte beschreiben die bekannten Probleme für den Siebel Connector:

SBL-Fehler beim Erstellen eines Kontos an mehreren Endpunkten

Eine Kontovorlage, die mehrere Endpunkte auflistet, kann nur Siebel-Gruppen anzeigen, die auf allen Endpunkten bestehen.

Kapitel 5: Behobene Probleme

Dieses Kapitel enthält folgende Themen:

12.6.1 (siehe Seite 63)

12.6.1

Die folgenden Probleme wurden in CA IdentityMinder 12.6.1 gelöst:

Support-Ticket	Berichtetes Problem
20576709/02	Unterstützung der Freigabe des gemeinsamen BusinessObjects Report Server sowohl für CA IdentityMinder als auch SiteMinder erforderlich
20576725/02	Unterstützung von BusinessObjects Report Server in einer Hochverfügbarkeitskonfiguration erforderlich
20583665/02	Unterstützung für BusinessObjects Report Server XI 3.1 SP5 (CABI 3.3) erforderlich
20774861/02	Fehler beim Einfügen von Daten sekundärer Objekte in Policy Xpress
20777137/02	Es wurden Verbesserungen am Richtlinien-basierten Workflow vorgenommen, bei dem sekundäre Objekte (Benutzerobjekte) abgerufen werden, die von primären Objekten benötigt werden.
20888199/01	DN-Namenskonvention für Kontovorlagen für TEWS nicht dokumentiert
21073146/01	"Synchronisieren von Konten mit Kontovorlage" synchronisiert nicht
21086870/01	Eigenständiges JCS-Installationsprogramm verlangt nicht nach Eingabe des FIPS-Schlüssels, was zu Problemen bei der Verschlüsselung führt
21108813/01	CA IdentityMinder 12.6 stellt nicht die erwarteten Rollendefinitionen bereit
21111634/01	JCS-Endpunktprotokolle werden nicht erstellt
21131768/01	Probleme mit dem Attribut für globalen Richtlinien-basierten Workflow (sekundärer Objekttyp fehlt für Ereignisdefinitionen)
21135604/01	Keine Anzeige der Aufgabe "Logical-Attribute-Handler" wegen NullPointer-Fehler
21136454/01	SQL-Injektions-Sicherheitsschwachstellen wurden in dieser Version beseitigt
21136456/01	Sicherheitsschwachstellen
21136499/01	Auswahlfelddaten funktionieren nicht bei einem Profil-Fenster, das in CA IdentityMinder 12.6 an einen Dienst angehängt ist
21137701/01	Ausnahme "PxEnvironmentException" wird empfangen, wenn Policy Xpress-Richtlinien externen Java-Code aufrufen

Support-Ticket	Berichtetes Problem
21140501-1	Unterstützung für Cloud-Bereitstellungen (Mandantenverwaltung)
21146621/01	Globale Attributvalidierung in "directory.xml"
21156269/01	Unterschiede zwischen den vom Installationsprogramm und den individuellen Datenbankskripten im Toolsordner generierten DB-Schemen
21156269/01	Mehr Skripte für manuelle Datenbankerstellung benötigt
21162602/01	Benutzerdefinierte Korrelation für TSS funktioniert nicht unter Unix
21170706/01	Ergebnisse der Aufgabe "Gesendet anzeigen" sind falsch sortiert, wenn Gebietsschema auf Dänisch eingestellt ist
21175201/01	Von eingehender Benachrichtigung initiierte Kontosynchronisierung wird nicht ausgeführt, wenn Bereitstellungsrollen mithilfe von Policy Xpress-Richtlinien zugewiesen werden
21181592/01	Fehler beim Laden von CA IdentityMinder r12.6 wegen ungültigem Klassenpfad
21183366/01	Falscher Benutzername bei Verwendung von Datenquellen
21187385/01	Wiederholte CA IdentityMinder-Abstürze
21188814/01	SiteMinder r12 SP3 CR11-Richtlinienserver stürzt ab, während auf CA IdentityMinder-Richtlinie zugegriffen wird
21190699/01	Abrufen sekundärer Objektinformationen durch Policy Xpress schlägt entweder bei Ereignis- oder Aufgaben-basierten Richtlinien fehl. Der ursprüngliche Attributwert wird auch zurückgegeben, sogar wenn Policy Xpress diesen nach Abschluss der Aufgabe entfernt.
21190873/01	508 Compliance-Problem: QuickInfos von Kontrollkästchen haben keine Bedeutung.
21193837/01	Erstellen und Löschen von verwalteten Objekten
21194712-1	Policy Xpress mit Iterator wird unterbrochen, wenn eine ausgelöste Zugriffsrollenzuweisung vom Workflow abgelehnt wird
21200396/01	508 Compliance-Problem: Link-Probleme bei "Zum Hauptinhalt wechseln"
21200412/01	508 Compliance-Problem: Warn- und Fehlermeldungen werden von Unterstützungssoftware für deaktivierte Benutzer nicht richtig gelesen.
21213029-1	Die im JSession-Zwischenspeicher gespeicherten Kennwortdienstvariablen werden nicht gelöscht (beim Abmelden), und nachfolgende Anfragen werden zur "pws.fcc"-Seite umgeleitet

Kapitel 6: Dokumentation

Die Dateinamen der CA IdentityMinder-Handbücher sind:

Handbuchname	Dateiname
Versionshinweise	im_release_deu.pdf
Implementierungshandbuch	im_impl_deu.pdf
Installationshandbuch für WebLogic	im_install_weblogic_deu.pdf
Installationshandbuch für WebSphere	im_install_websphere_deu.pdf
Installationshandbuch für JBoss	im_install_jboss_deu.pdf
Aktualisierungshandbuch	im_upgrade_deu.pdf
Konfigurationshandbuch	im_config_deu.pdf
Administrationshandbuch	im_admin_deu.pdf
Benutzerkonsolendesign-Handbuch	im_uc_design_deu.pdf
Programmierhandbuch für Java	im_dev_deu.pdf
Provisionierungs-Referenzhandbuch	im_provisioning_reference_deu.pdf
Connectors-Handbuch	im_connectors_deu.pdf
Handbuch für Connector Xpress	im_connector_xpress_deu.pdf
Implementierungshandbuch für Java Connector Server	im_jcs_impl_deu.pdf
Programmierhandbuch für Java Connector Server	im_jcsProg_deu.pdf
Glossar	im_glossary.pdf
Bookshelf	im_bookshelf_deu.zip

Dieses Kapitel enthält folgende Themen:

Bookshelf (siehe Seite 66)
Versionshinweise für CA IdentityMinder- und CA RCM-Integration (siehe Seite 66)

Bookshelf

Das Bookshelf ermöglicht den Zugriff auf die gesamte CA IdentityMinder Dokumentation über eine einzige Oberfläche. Folgende Funktionen sind enthalten:

- Erweiterbare Inhaltsangabe für alle Handbücher im HTML-Format
- Volltextsuche über alle Handbücher mit bewerteten Suchergebnissen und im Inhalt hervorgehobenen Suchbegriffen
- Klickelemente ("Brotkrümel"), die zu übergeordneten Themen führen
- Ein einziger HTML-Index für Themen in allen Handbüchern
- Links zu PDF-Versionen der Handbücher zum Drucken

So verwenden Sie den Bookshelf:

1. Laden Sie den Bookshelf von der Support-Website von CA herunter.
2. Entpacken Sie den Inhalt der komprimierten Bookshelf-Datei (.zip).

   Hinweis: Um eine bessere Leistung zu erhalten, sollten Sie, wenn Sie das Bookshelf auf einem Remote-System installieren, den Zugriff auf das Bookshelf über einen Webserver zulassen.
3. Zeigen Sie das Bookshelf wie folgt an:
   - Wenn sich das Bookshelf auf dem lokalen System befindet, und Sie Internet Explorer verwenden, öffnen Sie die Datei Bookshelf.hta.
   - Wenn sich das Bookshelf auf einem Remote-System befindet, oder wenn Sie Mozilla Firefox verwenden, öffnen Sie die Datei Bookshelf.html.

     Hinweis: Um eine bessere Leistung zu erhalten, sollten Sie, wenn Sie das Bookshelf auf einem Remote-System installieren, den Zugriff auf das Bookshelf über einen Webserver zulassen.

Zum Anzeigen des Bookshelfs ist Internet Explorer 7 oder 8 bzw. Mozilla Firefox 2 oder 3 erforderlich. Für die Links auf PDF-Handbücher ist Adobe Reader 7 oder höher erforderlich. Sie können Adobe Reader unter www.adobe.com herunterladen.

Versionshinweise für CA IdentityMinder- und CA RCM-Integration

Alle auf die Integration zwischen CA IdentityMinder und CA RCM bezogenen Versionshinweise befinden sich in den *Versionshinweisen für CA RCM*. Sie können auf das CA RCM-Bookshelf über CA Support zugreifen.

Anhang A: Barrierefreiheitsfunktionen

CA Technologies möchte sicherstellen, dass alle Kunden unabhängig von ihren Fähigkeiten die Produkte und die unterstützende Dokumentation erfolgreich einsetzen können, um damit zentrale Geschäftsaufgaben durchführen zu können. Dieser Abschnitt beschreibt die Eingabehilfen, die Teil von CA IdentityMinder sind.

508 Compliance

CA IdentityMinder ist konform mit Abschnitt 508 des US Rehabilitation Avt und den Web Content Accessibility Guidelines (WCAG2.0) auf AA-Ebene. Das Thema Produktverbesserungen (siehe Seite 67) bietet weitere Details. Sie können auch Ihren Account Manager nach einer Kopie des Voluntary Product Accessibility Template (VPAT) von CA Technology fragen.

Produktverbesserungen

CA IdentityMinder bietet Zugangsverbesserungen in den folgenden Bereichen:

- Anzeige
- Klang
- Tastatur
- Maus

Hinweis: Die folgenden Informationen beziehen sich auf Anwendungen unter Windows und Macintosh. Auf vielen Hostbetriebssystemen werden Java-Anwendungen ausgeführt, für die dort bereits Eingabehilfen verfügbar sind. Damit diese vorhandenen Eingabehilfen Zugriff auf Programme haben, die in JPL geschrieben sind, benötigen sie ein Bridge zwischen sich in ihren systemeigenen Umgebungen und der Java-Zugriffsunterstützung, die über die Java Virtual Machine (oder Java VM) verfügbar ist. Das eine Ende dieser Bridge ist in der Java VM und das andere auf der systemeigenen Plattform. So ist sie bei jeder Plattform unterschiedlich. Sun entwickelt gegenwärtig sowohl die JPL- als auch die Win32-Seite dieser Bridge.

Anzeige

Um die Sichtbarkeit auf Ihrer Computer-Anzeige zu vergrößern, können Sie die folgenden Optionen einstellen:

Schriftart, Farbe und Größe von Elementen

Ermöglicht die Auswahl der die Schriftartfarbe, der Größe und anderer visueller Kombinationen.

Bildschirmauflösung

Ermöglicht das Ändern der Pixelanzahl, um Objekte auf dem Bildschirm zu vergrößern.

Breite und Blinkrate des Cursors

Sorgt dafür, dass der Cursor leichter zu finden ist oder sein Blinken minimiert wird.

Symbolgröße

Ermöglicht das Vergrößern von Symbolen für bessere Sichtbarkeit oder das Verkleinern für mehr Bildschirmfläche.

Schemen für hohen Kontrast

Ermöglicht die Auswahl von Farbkombinationen, die besser zu sehen sind.

Klang

Verwenden Sie Klang als Alternative zur visuellen Darstellung oder um Computer-Klänge leichter hörbar oder unterscheidbar zu machen. Folgende Optionen können dazu angepasst werden:

Lautstärke

Ermöglicht das Erhöhen oder Verringern der Lautstärke des Computer-Klangs.

Text-zu-Sprache

Ermöglicht das Hören von Befehlsoptionen und Text durch laute Vorlesen.

Warnungen

Ermöglicht die Anzeige visueller Warnungen.

Hinweise

Gibt Ihnen akustische oder visuelle Zeichen, wenn Zugriffsfunktionen ein- oder ausgeschaltet werden.

Schemen

Ermöglicht die Zuordnung von Computer-Klängen zu bestimmten Systemereignissen.

Bezeichnungen

Ermöglicht die Anzeige von Bezeichnungen für Sprache und Klänge.

Hinweis: Wenn Sie ein Sprachausgabeprogramm verwenden, empfehlen wir, dass Sie die aktuelle Version des Tools für eine bessere Interpretation installieren.

Tastatur

Sie können die folgenden Tastaturanpassungen vornehmen:

Wiederholrate

Ermöglicht es einzustellen, wie schnell sich ein Zeichen wiederholt, wenn eine Taste gedrückt bleibt.

Töne

Ermöglicht die Ausgabe von Tönen, wenn bestimmte Tasten gedrückt werden.

Feststelltasten

Ermöglicht jenen, die mit nur einer Hand oder einem Finger tippen, alternative Tastaturlayouts auswählen.

Überspringen-Link

Ermöglicht die Nutzung des Links "Zum Hauptinhalt wechseln" für eine schnelle Navigation zum Hauptinhalt.

Maus

Sie können die folgenden Optionen verwenden, um Ihre Maus schneller zu machen und die Handhabung zu verbessern:

Klickgeschwindigkeit

Ermöglicht die Einstellung, wie schnell auf die Maustaste geklickt werden soll, um eine Auswahl zu machen.

Klicksperre

Ermöglicht das Hervorheben oder Ziehen, ohne die Maustaste gedrückt zu halten.

Umgekehrte Aktion

Ermöglicht das Umkehren der Aktionen, die über die linke und rechte Maustaste gesteuert werden.

Blinkrate

Ermöglicht die Einstellung, wie schnell der Cursor blinkt oder ob er überhaupt blinkt.

Zeigeroptionen

Ermöglicht Folgendes:

- Ausblenden des Zeigers während der Eingabe
- Anzeigen der Position des Zeigers
- Einstellen der Geschwindigkeit, mit der der Zeiger auf dem Bildschirm bewegt wird
- Auswählen der Größe und Farbe des Zeigers für bessere Sichtbarkeit
- Bewegen des Zeigers zu einer Standardposition in einem Dialogfeld

Ausnahmen bei Mozilla Firefox

Wir empfehlen, dass Tastaturbenutzer und JAWS-Benutzer aus folgenden Gründen den Internet Explorer 8 verwenden:

- In Firefox erhalten Dialogfelder den In/Out-Fokus nicht.
- In Firefox wird der Link "Zum Hauptinhalt wechseln" von der Sprachausgabe nicht immer zuerst vorgelesen.

Tastenkombinationen

Die folgende Tabelle listet die Tastenkombinationen auf, die CA IdentityMinder unterstützt:

Tastatur	Beschreibung
Ctrl+X	Ausschneiden

Tastatur	Beschreibung
Ctrl+C	Kopieren
Ctrl+K	Weitersuchen
Ctrl+F	Suchen und Ersetzen
Ctrl+V	Einfügen
Ctrl+S	Speichern
Ctrl+Shift+S	Alles speichern
Ctrl+D	Löschen der Zeile
Ctrl+Nach rechts	Nächstes Wort
Ctrl+Nach unten	Zeile nach unten scrollen
Ende	Ende der Zeile